計畫編號：NCCJ108-04

108 年委託研究報告

108 年度通訊傳播事業導入隱私保護管理機制與資料加值服務之研析委託研究採購案

期末報告─下冊

計畫委託機關：國家通訊傳播委員會

中華民國 109 年 3 月

計畫編號：NCCJ108-04

108 年委託研究報告

GRB 系統編號：PG108-05-0048

108 年度通訊傳播事業導入隱私保護管理機制與資料加值服務之研析委託研究採購案

期末報告—下冊

受委託單位

達文西個資暨高科技法律事務所

計畫主持人

葉奇鑫

研究人員

陳人傑、王慕民、吳彥欽、許博堯、蔡明德、郭麗靜

彭聖超、陳品安、洪郁雅、廖又萱、林廷憶

中華民國 109 年 3 月

下冊目錄

附件3：法規研究報告

壹、個人資料治理措施

一、個資保護長

（一）研究動機

依據我國個人資料保護法第 27 條第 1 項規定:「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」，又依據其施行細則第 12 條第 2 項第 1 款規定[1]，公務機關與非公務機關為達成之個人資料保護目的得配置管理之人員及相當資源。

惟本案與通傳業者共進行 25 場個資法遵輔導訪查，於訪查發現業者關於個資管理人員之問題如下：

1、 許多業者僅由各部門指定一名個資事宜管理人員出席訪查會議，於組織內部並無監督遵循個資保護事宜之專責人員。

2、 因各部門代表間缺乏可即時傳達資訊之管道，致不能即時彙整資料處理之現況，無法透過各部門之個資事宜管理人員代表充分了

[1] 臺灣，個人資料保護法施行細則，第 12 條，「本法第六條第一項但書第二款及第五款所稱適當安全維護措施、第十八條所稱安全維護事項、第十九條第一項第二款及第二十七條第一項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。前項措施，得包括下列事項，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：一、配置管理之人員及相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用之內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、使用紀錄、軌跡資料及證據保存。十一、個人資料安全維護之整體持續改善。」

解單一企業組織之整體資料處理作業情形。

3、無個資專責人員可即時提供內部相關專業意見並進行有效溝通。

為解決上述諸項問題，本研究將臚列歐盟一般資料保護規則（General Data Protection Regulation, GDPR）有關指派個資保護長（Data Protection Officers, 以下稱 DPO）之相關重要規範，以及歐盟第 29 條個人資料保護工作小組（Article 29 Data Protection Working Party，下稱 WP29）[2]於 2017 年發布《關於個資保護長之指引（Guidelines on Data Protection Officers，下稱 WP243 指引）》內容供委託機關參考。

（二）概述

GDPR 要求符合特定條件的資料控管者及受託者即有義務指派 DPO，此職位乃是歸責性的重要基礎，設置 DPO 職位可促進控管者與受託者內部的法規遵循，更能成為企業的競爭優勢。除了藉由歸責性工具（例如資料保護影響評估、執行稽核）促進法規遵循之外，DPO 也是各方利害關係人（主管機關、當事人以及控管者內部各業務單位）之間的中介者[3]。

（三）指派 DPO 的條件

依據 GDPR 第 37 條第 1 項規定，於三種情形下必須指派 DPO：

[2] 於歐盟 GDPR 在 2018 年施行後，WP29 的職責由歐洲個人資料保護委員會（European Data Protection Board, EDPB）取代，兩者任務均包含針對個人資料保護法律發布指引或意見。
[3] EU, WP29, *Guidelines on Data Protection Officers ('DPOs')*, WP243 rev.01, p.4.

於三種情形下必須指派 DPO：

1、 資料處理係由公務機關或機構為之。

2、 控管者或受託者之核心業務，包含須經常性、系統性對當事人進行大規模監控之處理作業。

(1) 核心業務（Core Activities）[4]

核心業務可視為達成控管者或受託者目標之關鍵性作業。而 GDPR 前言第 97 點明確指出，控管者之核心業務係指其「主要業務，與處理個資之附屬業務無關者」，於 GDPR 第 37 條第 1 項 b 款、c 款規定則說明，控管者或受託者之核心業務，包含依其本質、範圍及／或其目的，需要定期且系統性地大規模監控當事人，以及第 9 條所稱之大規模處理特殊類型之資料及第 10 條所稱之前科與犯罪相關之個人資料[5]。

(2) 大規模

依據 GDPR 第 37 條第 1 項 b 款、c 款規定，要求個資處理達到大規模程度，方符合須指派 DPO 之條件[6]。GDPR 對何謂大規模處理並無明確定義，可參考前言第 91 點，包含大規模使用新技術並用於

[4] EU, GDPR, §37(1)(b), "the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale;"
[5] EU, GDPR, §37(1)(c), " the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10."
[6] *Id.*

對當事人之權利與自由造成高風險之其他處理活動、利用剖析資料，就相關當事人之個人特徵為系統性、密集性之評估，或透過特殊類型之個人資料、生物資料、前科及犯罪資料或相關安全措施等[7]。而 WP29 則建議於判斷處理作業是否屬大規模作業時，應特別考量以下因素[8]：

A. 涉及之當事人數—是否達到一定數量或相關族群之一定比例

B. 處理之資料量及／或不同資料項目之範圍

C. 處理作業之時間長度或永久性

D. 處理作業之地理涵蓋範圍

屬於大規模處理作業的例子包含醫院一般作業對病患資料之處理、城市大眾運輸系統之個人旅行資料之處理（例如以票卡資料追蹤）、國際速食連鎖企業為統計目的，由專業之受託者對即時性之顧客地理位置資料之處理、保險公司或銀行一般作業對客戶資料之處理、搜尋引擎為投放行為廣告對個人資料之處理、電信或網路服務業之（內容、流量、位置）資料處理。

(3) 經常性且系統性之監控[9]

[7] EU, GDPR, Recital 97, "…for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures…"

[8] EU, WP29, *Guidelines on Data Protection Officers ('DPOs')*, WP243 rev.01, §2.1.3.

[9] EU, WP29, *Guidelines on Data Protection Officers ('DPOs')*, WP243 rev.01, §2.1.4.

經常性且系統性監控之概念於 GDPR 中並無定義，WP243 指引認為「經常性」係指具持續性或於一段時間內特定間隔發生、於固定時間反覆或重複發生、常態性或定時發生等。而「系統性」則為依據系統而發生、事先安排而有組織性或具一定方法為一套整體資料蒐集計畫之一部份、為一項策略執行之一部份。而 GDPR 前言第 24 點提及「監控當事人行為（to monitor of the behaviour of data subjects）」之概念時，明確將所有網際網路上之追蹤及建檔行為，包括分析或預測個人喜好、行為與態度[10]，均納入此範圍。然而，監控之概念並不限於網路上，線上追蹤也僅應視為對當事人監控的其中一例。

3、 控管者或受託者之核心業務，包含大規模處理特種資料或與刑事判決及罪刑相關之個人資料。

上述強制指派 DPO 之情形，於控管者及受託者皆有適用，換言之，只要符合上開強制指派 DPO 之要件，即應指派一名 DPO，且控管者與受託者所指派之 DPO 間應相互合作。惟須留意者，即使控管者符合強制指派 DPO 之標準，其受託者亦不必然須指派 DPO，即使未符合強制指派之要件，仍指派一名 DPO 則是較為周全之作法，而

[10] EU, GDPR, Recitals 24, "… In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."

無論組織係因強制或自願設置或指派 DPO，皆應符合 GDPR 第 37 條至第 39 條有關指派要件、職責及任務。

（四）數個組織指派一名 DPO[11]

GDPR 第 37 條第 2 項允許企業集團指派一名 DPO，而多個公務機關或機構於衡量其組織架構與規模後，亦可指派一個 DPO，此於 GDPR 第 37 條第 2、3 項定有明文。因考量 DPO 之任務之一為「向控管者、受託者及依此規則執行其處理作業之員工提供資訊及建議」，故 DPO 需以一種或數種語言有效率與當事人溝通，並與相關監管機關合作 (必要時可由團隊協助)。而控管者、受託者應確保無論於內部或外部，DPO 受多個公務機關或機構指派與否，皆可容易與 DPO 聯繫，此即 DPO 之「可及性（accessibility）[12]」。

（五）DPO 之可及性與所在位置[13]

WP243 指引建議無論控管者或受託者是否係設於歐盟境內，原則上 DPO 應設置於歐盟境內，但若因控管者或受託者於歐盟境內未設置據點，則 DPO 如設於歐盟境外更可有效執行業務，亦無不可。

（六）DPO 之專業及技能

DPO 之指派基礎為對個人資料保護法規之專業知識（包含深入了解國內法規、歐盟資料保護法規及實務專業等，如為公務機關或機

[11] EU, WP29, *Guidelines on Data Protection Officers ('DPOs')*, WP243 rev.01, §2.3.
[12] EU, GDPR, Section 4.
[13] EU, WP29, *Guidelines on Data Protection Officers ('DPOs')*, WP243 rev.01, §2.4.

構之 DPO，則應對該組織之行政規章及程序有全面且完善之瞭解），以及可確實達成 GDPR 第 39 條之任務之能力，WP243 指引認為此能力應解釋為個人特質、知識，個人特質則包含應具備誠信、高度之職業倫理，知識則包含資料處理原則、當事人權利、設計或預設之資料保護、處理作業紀錄以及資料外洩通知及溝通等 GDPR 中重要規範與原則之實施[14]。

惟 GDPR 對於「專業程度」之要求並無嚴格定義，視其所需執行之資料處理作業與所處理之資料應具備之保護措施為準，倘資料處理作業較複雜或涉及大量敏感性資料時，受指派之 DPO 應具備更高之專業程度。WP29 則建議 DPO 之指派應謹慎為之，並應適當參酌組織內產生之資料保護相關問題[15]。

（七）DPO 聯絡資訊之公布及傳播

依據 GDPR 第 37 條第 7 項規定要求控管者及受託者應公布 DPO 之聯絡資訊及細節，並將此聯絡資訊及細節提供予相關監管機關。

上開規定之目的係確保無論 DPO 所在位置為何處，當事人與監管機關皆無需透過組織之其他部門、人員，特別是組織員工，即得以簡易方式直接與 DPO 取得聯繫，而若聯繫者之身分無法保密，恐影響其向 DPO 申訴之意願。

[14] EU, WP29, *Guidelines on Data Protection Officers ('DPOs')*, WP243 rev.01, §2.5
[15] *Id.*

（八）DPO 之職位

GDPR 未明確要求於組織內必須設置一個名為「DPO」之具體職位，且依據 GDPR 第 37 條第 6 款規定[16]，DPO 可為控管者或受託者之員工或依服務契約由外部人員擔任並履行職務，若為後者，則須特別注意與組織成員是否有符合 GDPR 於第四節對於指派個資保護長之要求，例如應確認與組織成員間之任務與責任是否有利益衝突[17]。

然而無論由內部或外部人員擔任 DPO，控管者與受託者應確保 DPO 可「適切且即時地參與所有個資保護事宜」[18]，WP243 指引就個資保護事宜範圍舉例如下：定期參加組織內部管理高層及中階主管之會議、參與個資保護之決策進行、於發生資料外洩或其他事故時接受諮詢。且控管者與受託者應依處理作業之複雜度及敏感度，提供 DPO 相應之必要資源或其他服務管道（如人資、法務、資訊、資安等）之支援。

（九）DPO 之獨立性

為確保 DPO 可公正、客觀執行其任務，GDPR 賦予 DPO 一定程度之獨立性，例如 DPO 於執行其任務時，不得接受應如何處理事務之指示，亦不得接受應採特定見解之指示；且為強化 DPO 之自主性，

[16] EU, GDPR, §37(6), "The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract."
[17] EU, GDPR, §38(6), " The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests."
[18] EU, GDPR, §38(1), " The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data."

GDPR 規定 DPO 不因執行任務而受免職或處罰，此處罰包含各種直接或間接之形式，例如不予升遷或延遲升遷、阻礙職涯發展、不提供其他員工可得之福利等。且該處罰不須實際執行，僅是威脅將執行即構成 GDPR 禁止之行為。

又 GDPR 規定 DPR 應直接向最高管理階層彙報負責，以確保管理高層（例如董事會）知悉 DPO 於其職務範圍內提出之意見與建議事項，並可呈現於 DPO 提交最高管理階層的年度業務報告中。

最後，DPO 雖可執行其他任務或履行其他職責，但控管者應確保該任務或職責不得與 DPO 的職位產生利益衝突，即 DPO 不宜擔任內部可決定處理個人資料之目的及方式的職位例如執行長、營運長、財務長、行銷部主管、人資部主管、技術長等。

（十）DPO 之任務

1、 監督 GDPR 法律遵循事宜

依據 GDPR 第 39 條第 1 項規定，DPO 應協助、監督控管者及受託者遵循個人資料保護相關法規，如本規則、其它歐盟或會員國法之資料保護規定或控管者及受託者與個資保護相關之決策，然此監督法遵之任務，不代表 DPO 須承擔違法事件之責任，依 GDPR 第 24 條規定[19]，乃控管者應實施妥善之技術及組織性措施以確保並能舉證處

[19] EU, GDPR, §24(1), "… the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation."

理作業係依本規則辦理，是應由控管者負相關法律責任。

2、 監督資料保護衝擊影響評估之執行

於執行資料保護影響評估（Data Protection Impact Assessment，DPIA）時，DPO 應協助控管者執行 DPIA，提供相關建議，並依據 GDPR 第 35 條規定[20]監督 DPIA 之執行。

3、 與監管機關合作並作為聯絡點

依據 GDPR 第 39 條第 1 項第 d 款[21]、第 e 款[22]規定，DPO 應與監管機關合作，於資料處理議題，例如於資料保護影響評估之事前諮詢時，擔任監管機關之聯絡點，並於適當時提供其他事項之諮詢。

4、 對於風險之認知

DPO 於執行其職務時，應考量資料處理作業之本質、範圍、脈絡及目的，就此作業相關之風險具備應有之認識，此為 GDPR 第 39 條第 2 項之明文規定，WP243 指引對此亦說明[23]，該要求並非使 DPO 忽略監督風險較低之資料處理作業，而係應特別專注於風險較高之領域。此種選擇性且務實之方法，應可協助 DPO 就其執行 DPIA 應採取之方式、何種範圍應辦理內部或外部稽核、及應提供予負責資料處

[20] EU, GDPR, §39(1)(c), "to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;"
[21] EU, GDPR §39(1)(d), "to cooperate with the supervisory authority;"
[22] GDPR §39(1)(e)： "to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter."
[23] EU, WP29, *Guidelines on Data Protection Officers ('DPOs')*, WP243 rev.01, §4.4

理作業員工或管理階層何種內部訓練，及應投入其較多時間及資源於何種處理作業等事宜，向控管者提供諮詢意見。

5、 個資保護長於紀錄保存之角色

保留負責之資料處理作業紀錄或代控管者辦理之所有資料處理作業類別紀錄，依據 GDPR 第 30 條第 1 項[24]、第 2 項[25]規定，為控管者或受託者之責任，而非 DPO，惟由控管者或受託者就 DPO 負責之資料處理作業，指派其負責維護紀錄，亦無不可。

（十一）結論與建議

由歐盟 GDPR 相關條文及 WP243 指引可知，DPO 之職責如下：

1、 監督機關遵循國內、外之個人資料保護相關法律規範。

2、 對內負責稽核、教育訓練、提供資訊安全衝擊評估相關建議等。

3、 對外作為與主管機關聯繫之窗口。

因此，指派 DPO 不僅可使公務機關與非公務機關確保已採行資料保護之適當措施，並可降低資料外洩、資安事故之發生風險，亦可避免公務機關或非公務機關因違反個資保護相關規範而受罰，可見 DPO 之指派對於公務機關或非公務機關之重要性。且依 GDPR 第 3 條第 1 項適用範圍之規定[26]，我國電信業因提供國際漫遊、國際傳輸

[24] EU, GDPR, §30(1), "Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility…"
[25] EU, GDPR, §30(2), "Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller…"
[26] EU, GDPR, §30(1), "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the

等服務，其服務對象可能涉及歐盟境內資料當事人之個資，極可能成為 GDPR 適用之對象，故電信業實有指派個資保護長之必要。

又目前我國個人資料保護法並無如 GDPR 須強制指派個資保護長之要求，僅有公務機關應指定專人（第 18 條、施行細則第 25 條）與非公務機關應配置管理人員等（第 27 條第 1 項、施行細則第 12 條第 2 項第 1 款）規定[27]，惟非公務機關目前配置「管理人員」與 GDPR 所要求之個資保護長實有相當大的差異，且目前管理人員多由公司各部門指派一名個資事宜負責人員，其層級、職位、可及性、獨立性、專業能力均遠遠不及個資保護長，詳如下圖所示。

圖 1　管理人員與個資保護長之比較圖

	管理人員	個資保護長
可及性	不確定	有
獨立性	無	有
專業能力	不確定	有
風險認知	不確定	有
層級	低	高

processing takes place in the Union or not."

[27] 我國，個人資料保護法，第 18 條，「公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」、施行細則第 25 條：「本法第十八條所稱專人，指具有管理及維護個人資料檔案之能力，且足以擔任機關之個人資料檔案安全維護經常性工作之人員。公務機關為使專人具有辦理安全維護事項之能力，應辦理或使專人接受相關專業之教育訓練。」

面臨個人資料保護法修法在即，無論未來新法是否會參考 GDPR 增訂指派 DPO 之規定，如何即時因應現行法規與日後修法，並充分保護消費者之資料，確為主管機關與通傳業者皆應著重考量之問題，因此，建議委託機關可考慮以輔導、行政指導之方式，促請各業者分階段性完成指派 DPO 之要求，各階段目標如下，建請委託機關卓參。

1、 短期建議

(1) 落實現行個人資料保護法

依個人資料保護法第 27 條第 1 項、施行細則第 12 條第 2 項第 1 款規定，要求業者於公司內部設置管理人員。

(2) 加強內部個資相關法律遵循教育訓練

要求業者應定期安排內部員工應參與個人資料保護法律遵循教育訓練。

(3) 不定期輔導訪查

為確保業者遵循個人資料保護法規定，建議委託機關可不定期安排輔導訪查，以利隨時了解業者資料處理情況，並提供相關調適之建議。

2、 中期建議

(1) 擬訂指派個資專責人員之依據

建議委託機關可依據個人資料保護法第 27 條第 2、3 項之授權

（下同）[28]，要求非公務機關於「個人檔案安全維護計畫」增訂應指派專責人員負責個資相關事宜，且該專責人員應具備個資專業資格或證照。

(2) 個資專責人員應定期參與個資相關法律遵循教育訓練

承前，要求非公務機關應於「個人檔案安全維護計畫」增訂安排專任人員定期參與個資相關法律遵循教育訓練，以確保專責人員具備執行職務、任務之能力。

(3) 個資專責人員應不定期參與國內、國際學術講座及研討會

建議委託機關可輔導國內業者不定期參與國內、國際學術講座、研討會，以即時了解國際法規發展趨勢。

3、長期建議

(1) 要求業者指派高階專任人員／個資保護長

若個人資料保護法順利完成修法[29]，亦參照 GDPR 訂定個資保護長之規定，則委託機關應要求符合條件之業者指派相當於個資保護長職級之高階專任人員。

(2) 與高階專任人員／個資保護長保持即時聯繫管道

委託機關應確保業者已依法指派高階專任人員／個資保護長，並

[28] 臺灣，個人資料保護法，第 27 條第 2、3 項，「中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。」

[29] 台歐 11 月 27 日三度協商 GDPR 認定 國發會：個人資料保護法勢必修法，見 https://udn.com/news/story/7238/4188419，最後瀏覽日期：108 年 12 月 19 日。

要求業者與主管機關應保持可即時聯繫並進行有效溝通之管道。

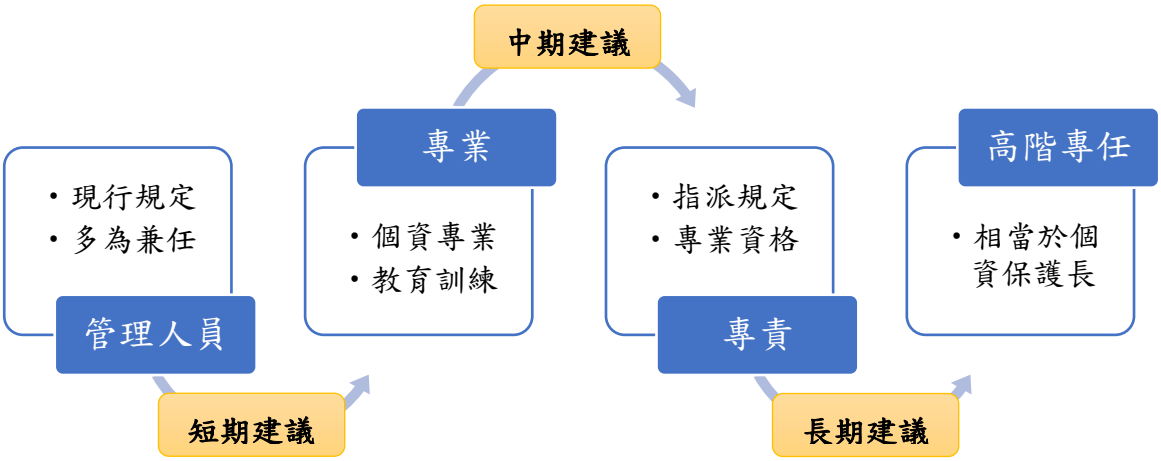


圖 2　個資專責（任）人員分階段性指派示意圖

二、個資保護影響評估

（一）研究動機

隨著大數據研究不斷發展，面對龐大資料量的處理與應用，透過「事前」的資料風險衡量、衝擊評估並提早規畫因應措施，以協助控管者管理事故產生之風險，乃目前國際趨勢，因此歐盟執行委員會廚於GDPR中規定DPIA外，並公布「資料保護影響評估指引（Guidelines on Data Protection Impact Assessment，簡稱DPIA指引）」，要求個人資料控管者依其進行個人資料衝擊評估，並建立一套有效檢視、評估並管理風險的管理制度。

又依據我國個人資料保護法第27條第1項[30]以及個人資料保護法施行細則第12條第2項第3款[31]，非公務機關保有個人資料檔案者得依適當比例為原則，進行個人資料之風險評估，然我國法對於應如何進行評估作業？未有具體規範。因此，本團隊認為DPIA指引應有其參考價值，故對其進行研究，並提出建議。

（二）歐盟資料保護影響評估指引

1、概述

歐盟執行委員會於2017年4月4日通過DPIA指引，DPIA是一種描

[30] 臺灣，個人資料保護法，第 27 條第 1 項，「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」

[31] 臺灣，個人資料保護法，第 12 條第 2 項，「前項措施，得包括下列事項，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：…三、個人資料之風險評估及管理機制…。」

述資料處理的程序，評估處理之必要性及符合比例原則，並透過評估個人資料[32]和確認因應問題之措施，以協助控管者管理因處理個人資料而對自然人權利和自由產生之風險。DPIA是課責制的重要工具，因DPIA不僅可協助控管者遵守GDPR之要求，亦可使控管者證明已採取適當措施確保遵守GDPR。換言之，DPIA是建立及證明合規性之程序。

依據GDPR，不遵守DPIA之要求可能導致權責監管機關之罰鍰。當處理須執行DPIA（第35條第1項和第3-4項）卻未能執行、未能以正確方式執行DPIA（第35條第2項和第7-9項）、或未依規定諮詢權責監管機關（第36條第3項第e款）時，可能導致高達1000萬歐元之行政罰鍰，或如為企業者，最高可達前一會計年度全球年營業額之百分之二，以金額較高者為準。

2、DPIA 指引之內容

與體現於GDPR中之風險基礎方法相符，DPIA並非對每個處理作業皆為強制性的。DPIA僅適用於當處理「可能對自然人之權利和自由造成高風險」時（第35條第1項）。為確保對強制性DPIA之情形作出一致性解釋（第35條第3項），DPIA指引首要目的即在於澄清此一概

[32] GDPR 並無正式定義 DPIA 本身之概念，然而第 35 條第 7 項規範其內容至少應包含：*(a)「對預計處理作業和處理目的之系統性描述，於適用情形下，包含控管者追求之合法利益；(b)與處理目的相關處理作業之必要性及符合比例原則之評估；(c)與第 1 項所述當事人權利和自由風險之評估；以及(d)為因應風險而預計採行之措施，包含維護措施、安全措施和機制，以確保個人資料之保護，並在考量到當事人和其他相關人員之權利和合法利益之情況下證明對本規則之遵守」*；前言第 84 點闡明其意義和作用為：「*當處理作業可能會對自然人之權利和自由造成高風險時，為了強化對本規則之遵守，控管者應負責執行資料保護影響評估，以檢視（尤其是）該風險之起源、性質、特殊性和嚴重性。*」

念，並為依據第35條第4項資料保護機關（DPAs）所應採用之清單提供標準。

3、DPIA 之目標

GDPR要求控管者採取適當措施以確保並能證明遵守GDPR，同時考量到「對自然人權利和自由造成各種可能和嚴重之風險」（第24條第1項）。控管者在某些情形下須執行DPIA之義務應從其須適當管理個人資料處理風險[33]之一般義務的角度來理解。

「風險」是描述依據嚴重性和可能性進行估算的事件及其後果之可能情境。另一方面，「風險管理」可被定義為指導和控制組織中與風險相關之協調活動。

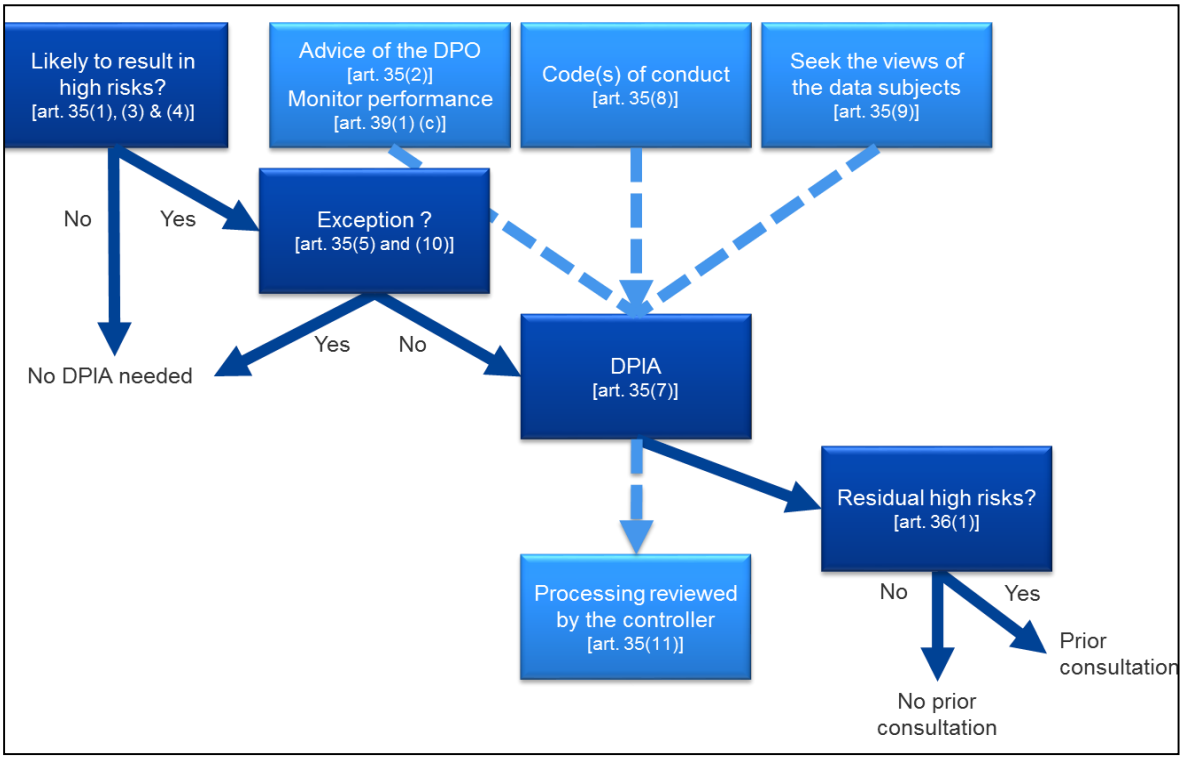
第35條適用於「對個人之權利和自由」可能存在高風險之情況。如第29條資料保護工作組關於風險基礎方法在資料保護法律架構中之作用的聲明所述，當事人之「權利和自由」主要考量的是資料保護和隱私之權利，然亦可能涉及其他基本權利，如言論自由、思想自由、行動自由、禁止歧視以及自由、良心和宗教之權利。

依據GDPR風險基礎方法，DPIA並非對每個處理作業皆為強制性的。相反的，僅有當處理個人資料涉及「可能對自然人之權利和自由

[33] It has to be stressed that in order to manage the risks to the rights and freedoms of natural persons, the risks have to identified, analyzed, estimated, evaluated, treated (e.g. mitigated...), and reviewed regularly. Controllers cannot escape their responsibility by covering risks under insurance policies.
必須強調的是，為了管理自然人權利和自由之風險，必須確認、分析、預估、評估、因應（例如減輕...）風險，並定期審查。控管者不得透過承保契約來規避風險管理之責任。

造成高風險」時才需要DPIA（第35條第1項）。然而，未滿足觸發執行DPIA義務之事實並不會減少控管者應實施對當事人權利和自由的適當風險管理措施之一般義務。在實務上，此意味著控管者必須不斷評估其處理活動所產生之風險，以確認何種類型之處理「可能對自然人權利和自由造成高風險」。下圖說明GDPR中與DPIA之基本原則：

圖表 1：GDPR 中與 DPIA 之基本原則[34]



4、DPIA 之適用範圍

DPIA可僅涉及單一資料處理作業。然而，第35條第1項規定「單一評估可針對一系列類似且呈現相似高風險之處理作業」。前言第92點補充說明「在某些情況下，資料保護影響評估之標的不限於單一計

[34] EU, Guidelines on Data Protection Impact Assessment (DPIA) , determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, p.7。

畫，是屬較合理且經濟的，例如，當公務機關或機構欲建立共同的應用程式或處理平台，或當數個控管者計畫引進共同的應用程式或跨產業或跨界之處理環境，或為廣泛使用的水平整合活動」[35]。

一份DPIA可用於評估在性質、範圍、背景、目的和風險方面類似之數個處理作業。實際上，DPIA旨在系統性的研究對自然人權利和自由可能造成高風險之新情況，因此對已經研究過的案例（例如在特定情況和特定目的下進行之處理作業）即無執行DPIA之必要性。此種情況可能係使用類似之技術並基於相同之目的蒐集相同種類之資料。例如，當市政當局的各機關獨自建立類似之CCTV系統時，可執行一份DPIA，涵蓋不同控管者的處理作業，或是鐵路運營商（單一控管者）可在一份DPIA中涵蓋其所有車站的影音監視。此亦可能適用於由不同資料控管者實施類似處理作業之情形。於此情況下，所提供之DPIA應被共享或可公開取得，DPIA中描述之措施必須被實施，且須提供執行單份DPIA之理由。[36]

---

[35] *Id*.
A DPIA may concern a single data processing operation. However, Article 35(1) states that "a single assessment may address a set of similar processing operations that present similar high risks". Recital 92 adds that "there are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity".

[36] *Id*.
A single DPIA could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks. Indeed, DPIAs aim at systematically studying new situations that could lead to high risks on the rights and freedoms of natural persons, and there is no need to carry out a DPIA in cases (i.e. processing operations performed in a specific context and for a specific purpose) that have already been studied. This might be the case where similar technology is used to collect the same sort of data for the same purposes. For example, a group of municipal authorities that

當處理作業涉及共同控管者時，需精確地定義其各自之義務。DPIA中應指明哪一方負責處理風險及保護當事人權利和自由之各種措施。每個資料控管者皆應表達其需求並分享有用資訊，但不至洩露秘密（例如：保護商業秘密、智產權，商業機密資訊）或揭露弱點。[37]

DPIA亦可用於評估技術產品(例如硬體或軟體產品)對資料保護之影響,這可能被用於不同的資料控管者實施不同處理作業時。當然，使用該產品之資料控管者仍有義務就具體實施方面執行自己的DPIA，但可於適當情形下使用由產品供應商準備之DPIA。智能電錶製造商和公用事業公司間之關係可提供示例。每個產品提供者或受託者應共享有用資訊，但不至洩露秘密，亦不至因揭露弱點導致安全風險。[38]

---

are each setting up a similar CCTV system could carry out a single DPIA covering the processing by these separate controllers, or a railway operator (single controller) could cover video surveillance in all its train stations with one DPIA. This may also be applicable to similar processing operations implemented by various data controllers. In those cases, a reference DPIA should be shared or made publicly accessible, measures described in the DPIA must be implemented, and a justification for conducting a single DPIA has to be provided.

[37] *Id.* at 7-8.

When the processing operation involves joint controllers, they need to define their respective obligations precisely. Their DPIA should set out which party is responsible for the various measures designed to treat risks and to protect the rights and freedoms of the data subjects. Each data controller should express his needs and share useful information without either compromising secrets (e.g.: protection of trade secrets, intellectual property, confidential business information) or disclosing vulnerabilities.

[38] *Id.* at 8.

A DPIA can also be useful for assessing the data protection impact of a technology product, for example a piece of hardware or software, where this is likely to be used by different data controllers to carry out different processing operations. Of course, the data controller deploying the product remains obliged to carry out its own DPIA with regard to the specific implementation, but this can be informed by a DPIA prepared by the product provider, if appropriate. An example could be the relationship between manufacturers of smart meters and utility companies. Each product provider or processor should share useful information without neither compromising secrets nor leading to security risks by disclosing vulnerabilities.

5、 應執行 DPIA 之標準

GDPR不要求每個可能造成自然人權利和自由風險之處理作業皆需執行DPIA。只有當處理「*可能對自然人權利和自由造成高風險*」之情況下才必須執行DPIA（第35條第1項，第35條第3項加以闡明，並由第35條第4項補充）。此規定在引入新的資料處理技術時尤為重要[39]。若不確定是否需執行DPIA，WP29建議仍執行DPIA，因DPIA係協助控管者遵守資料保護法的有效工具。

為了提供一套因其固有之高風險而需執行DPIA之更具體的處理作業，並考量到第35條第1項和第35條第3項第a至c款之特定要件、第35條第4項和前言第71、75和91點應於國家層級制定之清單、以及其他GDPR規範所提及「*可能造成高風險*」之處理作業[40]，應考量以下九項標準。

(1) 評估或評分。包含剖析和預測，尤其是關於當事人工作表現、經濟狀況、健康、個人偏好或興趣、可信度或行為、位置或行動等面向。

(2) 具有法律效果或類似重大影響之自動化決策。當處理目的是為做出有關當事人之決定，且該決定產生「關於該自然人之法律效果」或該決定「類似重大影響該自然人」。

[39] EU, Recitals 89, 91 and Article 35(1) and (3) , further examples.
[40] EU, Recitals 75, 76, 92, 116, further examples.

(3) 系統性監控。用於觀察、監測或控制當事人之處理，包括透過網路蒐集之資料或「於公眾開放區域進行系統性之監控」。

(4) 敏感資料或高度私人性質資料。此類資料包括第9條中定義之特殊類型個人資料（例如有關個人政治觀點之資訊），以及與第10條中定義之刑事定罪或犯罪相關個人資料。例如綜合醫院保存病人醫療記錄或私人調查員保留違法者之詳細資訊。

(5) 大規模資料處理。綜合考量當事人之數量、資料數量或處理不同資料項目之範圍、資料處理活動之持續時間以及處理活動的地域範圍。

(6) 配對或組合資料集41。例如處理不同目的或不同資料控管者的資料，且其方式將超出當事人之合理期待。

(7) 與弱勢當事人相關之資料。處理此類型資料成為標準係因當事人和資料控管者間權力不平衡增加，此意味著當事人可能無法輕易地同意或拒絕其個人資料之處理或行使其權利。

(8) 創新使用或應用新的技術性或組織性之解決方案。例如結合使用指紋和臉部識別以改進實體存取控制等。

(9) 當處理本身「阻止當事人行使權利或使用服務或契約」時。此情形包括目的在允許、修改或拒絕當事人取得服務或簽訂契約之處

41 EU, WP29, Opinion on Purpose limitation 13/EN WP 203, p.24.

理作業。

6、DPIA 適用評估之範例

以下示例說明如何使用前述標準評估一個特別的處理作業是否需要DPIA[42]。

處理之示例	可能相關標準	是否需要DPIA？
● 醫院處理病患之基因和健康資料（醫院資訊系統）。	● 敏感資料或高度私人性質資料。 ● 與弱勢當事人相關之資料。 ● 大規模資料處理。	是
● 使用攝影系統監控高速公路上的駕駛行為。控管者預計使用智能影像分析系統來挑選車輛並自動識別車牌。	● 系統性監控。 ● 創新使用或應用新的技術性或組織性之解決方案	
● 公司系統性地監控員工活動，包括監控員工的個人工作區、網路活動等。	● 系統性監控。 ● 與弱勢當事人相關之資料。	
● 蒐集公眾社交媒體資料以建立剖析檔案。	● 評估或評分。 ● 大規模資料處理。 ● 配對或組合資料集。 ● 敏感資料或高度私人性質資料。	
● 建立國家層級的信用等級或詐欺資料庫之機構。	● 評估或評分。 ● 具有法律效果或類似重大影響之自動化決策。 ● 阻止當事人行使權利或使用服務或契約。 ● 敏感資料或高度私人性質資料。	
● 基於歸檔目的儲存用於研究項目或臨床試驗之弱勢當事人的假名化個人敏感資料。	● 敏感資料。 ● 與弱勢當事人相關之資料。 ● 阻止當事人行使權利或使用服務或契約。	

[42] EU, 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, p.11-12.

處理之示例	可能相關標準	是否需要DPIA？
● 由「個人醫生、其他健康照護專業人員或律師」處理「病患或客戶之個人資料」。	● 敏感資料或高度私人性質之資料。 ● 與弱勢當事人相關之資料。	否
● 網路雜誌使用郵件列表向其訂閱戶發送一般每日摘要。	● 大規模資料處理。	
● 電子商務網站基於在其網站上查看或購買項目的有限剖析檔案，顯示經典汽車零件的廣告。	● 評估或評分。	

（三）我國個人資料保護法對衝擊評估之相關規定

我國關於風險管理之相關規定，在於個人資料保護法第6條第1項但書第2款及第5款、第18條、第19條第1項第2款及第27條第1項所稱之適當安全措施以及適當安全維護措施，而所謂安全維護事項以及適當安全措施可參考個人資料保護法施行細則第12條第2項列舉項目，包括一、配置管理之人員及相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用之內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、使用紀錄、軌跡資料及證據保存。十一、個人資料安全維護之整體持續改善，等11項措施。

各目的事業主管機關為有效管理本身組織及轄下單位落實個人資料保護法所規範之安全維護措施，可對上述11項措施項目進一步提出實行架構，以經濟部為例，並於107年3月制定「經濟部個人資料保

護作業手冊[43]」並持續更新，其中便包含制定個人資料風險評估作業程序，要求經濟部各單位及所屬機關應規劃個人資料風險評估與管理作業，風險評估作業應包括下列項目：

1、 評估個人資料風險

(1) 風險評估單位及所屬機關應使用個人資料風險評估表就個人資料檔案內容進行價值識別。個人資料之價值識別得以個人資料之內容、個人資料之數量、個人資料檔案之識別程度，以及其他必要之項目為評估基準。

(2) 於個人資料檔案內容價值識別後，應進行個人資料作業之具體風險類型識別。

(3) 就識別出之風險，風險發生之衝擊程度及發生之可能性進行風險評估並區分等級。風險發生之衝擊程度得以損害高低以及其他必要之項目為評估基準。

(4) 就風險發生之衝擊程度及發生之可能性進行識別後，應予以區分風險等級，並就高風險之個人資料檔案作業進行風險處理。

2、 處理個人資料風險

依風險評估結果進行風險處理，擬定具體對策。

[43] 經濟部個人資料保護作業手冊 107 年 3 月版(10802 更新)，https://www.moea.gov.tw/MNS/colr/content/SubMenu.aspx?menu_id=7783

3、 建立風險評估清冊

風險評估單位及所屬機關應將風險評估之結果製作個人資料風險評估清冊，並妥善保管且定期維護該清冊。

該程序不僅應依個人資料之價值、風險發生之衝擊程度及發生之可能性進行風險評估，並應依風險評估結果進行風險處理，擬定具體對策，同時應建立並定期維護風險評估清冊[44]。該作業程序中亦提供了可實際操作之風險情境表[45]與個資流程衝擊分析表[46]，作為單位執行風險評估時之參考。

該風險情境表將風險情境分為紙本類、電子類，系統資料庫類以及委外作業類，並在各分類下進一步細分子分類之風險細項以及個資潛在風險事件。例如常見的系統資料庫就區分為存取權限與使用紀錄兩個風險評估子分類，而潛在風險事件則包含了資訊系統之使用者帳號均定期審查、依據職務區隔之存取權限、活動日誌記錄功能以及定期審查日誌記錄等；個資流程衝擊分析表也針對個資作業流程列舉衝擊分析的主要項目，其中包括個資數量、個資敏感度、損害組織信譽、個資當事人隱私衝擊等四大面項，並將各面項可能產生之衝擊分為1、3、5三種量化衝擊程度之數值，最後將各流程中的衝擊數字加總作為

[44] 同前註，第 12 頁以下。
[45] 風險情境表(10802 更新)，https://www.moea.gov.tw/MNS/COLR/content/wHandMenuFile.ashx?file_id=19967。
[46] 個資流程衝擊分析表，https://www.moea.gov.tw/MNS/COLR/content/wHandMenuFile.ashx?file_id=17630。

該作業流程對隱私衝擊之具體評估分數，以供組織決策參考。

風險情境表[47]

風險大分類	風險子分類	個資潛在風險事件
1.紙本類	1.1 處理	1.1.1 紙本文件於內部處理過程中，長時間不使用或下班時收存於辦公室上鎖之資料櫃。
	1.2 保存	1.2.1 紙本文件之保存(含暫存區)地點具備進出管控措施。
		1.2.2 紙本文件歸檔、入倉(庫)或集中保管前，確實清點數量及內容。
		1.2.3 紙本文件存放地點有消防、滅火、溫度控制等設施。
	1.3 傳遞	1.3.1 紙本文件於內部傳遞過程中，具有簽收/點收等控管措施。
		1.3.2 紙本文件提供外部利用均有公文往返等使用紀錄。
	1.4 銷毀	1.4.1 包含個資之紙本文件均不進行回收使用。
		1.4.2 紙本文件於內部進行銷毀時，均銷毀致無法辨識。
		1.4.3 紙本文件交由受委託廠商銷毀前，已簽訂包含雙方權利義務及賠償條款之契約或保密協議。
		1.4.4 紙本文件交由受委託廠商進行銷毀時，妥善進行監銷並留存紀錄。
2.電子類	2.1 傳輸	2.1.1 同仁透過對外寄發、傳輸個資檔案均進行加密。
		2.1.2 同仁對外傳輸個資檔案均有傳輸記錄，如 Email 寄件備份、FTP 傳輸記錄、網路硬碟等。
	2.2 保存	2.2.1 存於本機電腦之個資檔案，均有加密或存放於專用且安全之資料夾。
	2.3 銷毀	2.3.1 電子檔案保存期限屆滿後均進行刪除。
3. 電子檔 - 可攜式媒體	3.1 傳遞	3.1.1 將個人資料檔案使用可攜式媒體傳遞時，均進行加密。
	3.2 銷毀	3.2.1 儲存個人資料之可攜式媒體不再使用或損毀

[47] 同註 45。

		時，均進行刪除資料或實體破壞。
4.系統資料庫	4.1 存取權限	4.1.1 資訊系統之使用者帳號均定期審查。
		4.1.2 系統具備職務區隔機制，給予適當之存取權限。
	4.2 使用紀錄	4.2.1 資訊系統具有記錄使用者活動日誌功能。
		4.2.2 單位主管或其授權人員定期審查資訊系統使用者之活動日誌。
5.委外作業類	5.1 選商	5.1.1 委外案件均會評估及選擇可提供符合組織對個人資料保護需求之受委託廠商(如一年內未曾發生個資外洩事件、重大資安事件或有無通過 ISO 27001、BS10012、TPIPAS、ISO29100 等驗證)。
	5.2 簽約	5.2.1 在委託外部單位處理個人資料有簽訂契約，並包含適當安控措施是否足夠。
		5.2.2 組織與受委託廠商所簽訂之契約中包含是否得將個人資料處理作業進行轉包/分包之規定。
		5.2.3 若允許轉包/分包，受委託廠商與其複委託廠商(下包商)所簽訂之契約已要求複委託廠商實行與受委託廠商相同等級之安控措施。
		5.2.4 組織與受委託廠商所簽訂之契約中明確規範，當資料逾保存期限或契約終止時，有關個人資料之銷毀、交還原組織或其他處理方式。
	5.3 履約	5.3.1 於委託外部單位處理個人資料契約期間內，定期監督或實地審查受委託廠商之安控措施是否落實執行。
		5.3.2 組織定期依據與受委託廠商所簽訂之契約進行監督，當資料逾保存期限或契約終止時確認有關個人資料之銷毀、交還原組織或其他處理之方式。
	5.4 小額採購	5.4.1 如以小額採購方式委託外部單位蒐集、處理、利用或銷毀個人資料時，均簽訂書面協議並落實監督作業。

個資流程衝擊分析表[48]（範例）

作業流程名稱		衝擊分析項目				衝擊值		
主要業務、職掌	細部作業名稱	個資數量	個資敏感度	損害組織信譽	個資當事人隱私衝擊	衝擊值係以衝擊構面之評分加總	備註	單位名稱
		5:每年產生大於1000筆	5:包含姓名、身分證號、私人連絡方式(電話+地址)、財務情況、指紋、特種個資	5:若作業發生個資外洩事故，將導致機關形象、信譽受到非常嚴重損害，如：導致國際性媒體報導負面新聞、造成民眾集結遊行抗爭或上級機關關切等情形。	5: 洩漏資訊，對個資當事人造成重大影響，如:勒索、綁架。			
		3:每年產生100~1000筆	3:包含姓名、身分證號、護照、私人聯絡方式(電話及地址)、其他非特種特資欄位	3:若作業發生個資外洩事故，將導致機關形象、信譽受到嚴重損害，如：導致3家以上媒體報導負面新聞或造成民眾至機關抗議或陳情等情形。	3: 洩漏資訊，對個資當事人有部分影響，如:遭受不明騷擾、詐騙。			
		1:每年產生小於100筆	1:僅含姓名、聯絡方式(電話)	1:若該作業發生個資外洩事故，將導致機關形象、信譽受到輕微損害，如：導致部份媒體報導負面新聞、造成多位民眾電話抱怨等情形。	1: 洩漏資訊，對個資當事人產生些微影響			

（四）結論與建議

GDPR並未強制所有個人資料蒐集主體都應依照DPIA指引規定進行衝擊評估，是否需要依照DPIA指引規定進行衝擊評估應依下列九項標準進行評估：

1、 評估或評分。

[48] 同註 46。

2、 具有法律效果或類似重大影響之自動化決策。

3、 系統性監控。

4、 敏感資料或高度私人性質資料。

5、 大規模資料處理。

6、 配對或組合資料集 。

7、 與弱勢當事人相關之資料。

8、 創新使用或應用新的技術性或組織性之解決方案。

9、 當處理本身將阻止當事人行使權利、使用服務或締結契約。

國家通訊傳播委員會職掌全國通訊傳播事業、通訊傳播平臺事業設立及網路營運之監督管理[49]，本研究範圍之電信業者、有線電視業者，其所蒐集、處理及利用之個人資料不僅資料處理規模龐大、不同類型資料相互配對處理之實例所在多有，且資料中不乏具有高度敏感性與私人性質的資料，在可預見的未來都有機會就蒐集之個人資料進行大規模資料處理或創新使用，依照DPIA指引應否適用DPIA的九大標準，上開業者現行或未來規劃之個人資料作業流程均可能有進行衝擊評估之必要。因此，雖然我國個人資料保護法並未強制資料蒐集主體應進行個人資料衝擊評估作業，本團隊仍建議國家通訊傳播委員會可依據產業特性，建立個人資料衝擊評估作業程序，以供轄下電信業

[49] 國家通訊傳播委員會平台事業管理處職掌，
https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=5170&sn_f=41727。

者、有線電視業者遵行。

本研究建議可參考下列方向建立個人資料衝擊評估作業程序：

1、 法源依據

(1) 以特別法為法源依據

電信管理法第15條第1項規定：「設置使用電信資源之公眾電信網路之電信事業或其他經主管機關公告之電信事業，應訂定資通安全維護計畫，並依該計畫實施。」同條第2項規定：「第一項主管機關公告電信事業之考量因素、前項資通安全管理範圍、分級、驗證基準、程序、聯防應變通報作業及其他應遵行事項之辦法，由主管機關定之。」由於個人資料衝擊評估作業有相當程度之範疇屬資通安全管理範圍，且該法之法律效果明確[50]，可有效要求業者遵循，但個人資料衝擊評估作業除資通安全管理範圍外，仍有諸多法規遵循要求（例如：應行告知事項、取得當事人同意），若以其為法源依據規範業者，恐有逾越法律授權之虞。

(2) 以個人資料保護相關法規為法源依據

依據我國個人資料保護法第27條第1項[51]以及個人資料保護法施行細則第12條第2項第3款[52]，國家通訊傳播委員會定有「國家通訊傳

[50] 臺灣，電信管理法，第 79 條，「電信事業有下列情形之一者，處新臺幣十萬元以上一百萬元以下罰鍰，並通知限期改正；屆期未改正者，得按次處罰：...十三、違反第十五條第一項規定，未訂定資通安全維護計畫或未按計畫實施...。」

[51] 同註 30。

[52] 同註 31。

播委員會指定非公務機關個人資料檔案安全維護辦法」，並要求其轄下業者訂定個人資料檔案安全維護計畫，依其法律授權不僅得要求業者進行個人資料衝擊評估作業，且作業範圍應可包含資通安全管理以及法規遵循要求，然而該辦法現行內容並未要求轄下業者進行個人資料衝擊評估作業。

(3) 衡量上述二法源依據之利弊得失，因以特別法為法源依據規範業者，恐有逾越法律授權之虞，且電信管理法修正須經立法院三讀通過，難度較高，反觀「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」之修正門檻較低。因此，建議將個人資料衝擊評估作業納入該辦法，以作為業者遵循依據。

2、界定規範對象與範圍

GDPR其亦未強制所有個人資料蒐集主體都應依照DPIA指引規定進行衝擊評估，建議國家通訊傳播委員參考前述DPIA指引之九大標準，規範應進行個人資料衝擊評估作業之業者標準及作業流程標準，並明訂於「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」。

3、制定個人資料衝擊評估作業程序指引

國家通訊傳播委員會轄下電信業者、有線電視業者，其個人資料蒐集、處理與利用流程相較其他產業有其特殊性，且同類業者間又有

其相似性，建議國家通訊傳播委員會可參考經濟部做法，制定切合電信業者、有線電視業者之個人資料衝擊評估作業程序指引，以供相關業者遵行。

4、依比例原則輔導業者完成評估作業

本團隊於本委託案進行期間發現，各業者間因營運規模差異甚大，其法規遵循與資安管理能量均有不同，齊頭式要求業者進行全面性個人資料衝擊評估作業，恐怕窒礙難行。因此，建議國家通訊傳播委員會得以行政指導方式輔導中小型業者，依其規模需要進行衝擊評估作業，以符合現實需要。

貳、當事人權利—資料可攜權

一、研究動機

歐盟於一般資料保護規則（General Data Protection Regulation，GDPR）第20條[53]中創造了一種新的資料可攜權，此種權利與存取權有著相當密切之關係，但同時又有著許多不同之處。參照GDPR第20條之內容可知，資料可攜權允許當事人得以結構性、一般性及機器可讀性之格式，接收其提供予資料控管者之個人資料，並將此等資料傳輸至另一資料控管者，而此項新權利創設之目的，係為賦予當事人能更有效且自主性地掌控與自身相關個人資料之權利；由於資料可攜權允許將個人資料從一資料控管者直接傳輸至另一資料控管者，因此該權利亦是促使歐盟各會員國間個人資料之自由流通及促進資料控管者競爭之重要工具；資料可攜權亦可增進不同服務提供商之間之轉換，並從而促進在數位單一市場下開發新服務。

緣目前我國個人資料保護法就資料可攜權尚未有明文規定，又資

[53] EU, GDPR, §20, "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and the processing is carried out by automated means.
In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
1The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. 2That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.".

料可攜權於現今科技發達、數位化蓬勃發展之年代而顯得日益重要，故特此以GDPR第20條資料可攜權為研究標的。

二、歐盟資料可攜權

（一）資料可攜權之目的

資料可攜權僅適用於由當事人提供之個人資料，此權利不得以任何方式被侵害，且當事人提供其個人資料並不僅限於以直接、傳統或書面之方式傳達，而得以其他間接或電子化等方式提供，例如，填寫線上表格等[54]。在符合特定要件下，資料可攜權賦予當事人選擇、控制及授權之權利（詳如後述），過去資料之可攜性會受限於資料控管者在提供當事人請求資訊之格式，而新的資料可攜權則賦予了當事人就自身個人資料之多項能力，該權利有助於當事人輕易地將其個人資料從一個IT環境中移動、複製或傳輸至另一個IT環境[55]。資料可攜權亦再平衡了當事人及資料控管者之間的關係，使資料控管者及當事人間不再是上對下的關係，當事人能親自掌控自己的個人資料。資料可攜權之主要目的係增強當事人對其個人資料之控制，並確保其在資料系統中扮演積極之角色，雖然個人資料可攜權可以因為當事人能輕易將其個資轉換而增加服務間之競爭，但GDPR所欲規範的是個人資料

[54] EU, WP29, Guidelines on the right to data portability, "…This new right cannot be undermined and limited to the personal information directly communicated by the data subject, for example, on an online form...", p.3.
[55] EU, WP29, Guidelines on the right to data portability, P."…The new right to data portability aims to empower data subjects regarding their own personal data, as it facilitates their ability to move, copy or transmit personal data easily from one IT environment to another...", p.4.

而非市場競爭，特別是GDPR第20條並未將可攜資料限縮於為轉換服務所必需或有用之資料。

（二）資料可攜權之權利內涵

1、 接收個人資料之權利

資料可攜權是一種當事人接收由資料控管者處理之相關個人資料，並為進一步個人使用而儲存此些資料之權利。此種儲存可以是在私人設備或私人雲端上，不一定需將資料傳輸至另一資料控管者，在此情形下，資料可攜權補充了存取權，資料可攜權的其中一個特點即在於為當事人提供了一種簡單的方式來管理和再使用個人資料[56]。

2、 傳輸至另一控管者之權利

GDPR第20條第1項[57]規定當事人有權利「不受妨礙地」將其個人資料從一資料控管者傳輸至另一資料控管者，在技術可行之前提下，原資料控管者依據當事人之請求，更可將該該當事人之個人資料直接從一資料控管者直接傳輸至另一資料控管者(GDPR第20條第2項[58])。

[56] 達文西個資暨高科技法律事務所，「GDPR 相關指引文件研析」委託研究計畫，國家發展委員會，2019 年。。

[57] GDPR §20(1)"The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
the processing is carried out by automated means."

[58] GDPR §20(2)"In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.".

鑑此，GDPR前言第68點[59]鼓勵資料控管者建立互通之格式，以便於實現資料可攜權（便於服務間資料之轉換），但GDPR禁止控管者設置傳輸障礙，意即資料控管者無建立共通系統之義務，但禁止妨礙傳輸當事人之個人資料。基本上，此種資料可攜權之要素不僅為當事人提供了取得及再使用自身資料之權利，亦使其可就所提供之資料傳輸予另一服務提供商（無論是否在同一產業類別內）。除了透過賦予消費者權利以防止「被鎖在」單一服務提供商（如前述資料控管者及當事人間權力、資訊、技術不對等之情形），資料可攜權被預期可在當事人控制下，以安全可靠之方式促進與其他資料控管者間個人資料共享及再使用之機會。

[59] EU, GDPR, Recital §68, " To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. 2Data controllers should be encouraged to develop interoperable formats that enable data portability. 3That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. 4It should not apply where processing is based on a legal ground other than consent or contract. 5By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. 6It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. 7The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. 8Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. 9Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. 10Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another."

3、 控制權

(1) 控管者不限於同產業內：

資料可攜權確保當事人得依據其意願接收及處理個人資料之權利，且此權利不僅限於對與資料控管者提供類似服務之競爭者（即不論是否在同一產業類別內）有用且相關之個人資料。

(2) 資料控管者無須對當事人或接收個人資料之其他公司就該資料之處理負責

資料控管者在依據GDPR第20條規定之要件回應當事人之資料攜帶請求時，無須對當事人或接收個人資料之其他公司（即另一資料控管者）就該資料之處理負責。資料控管者代表當事人行事，包括將個人資料直接傳輸至另一資料控管者。於此情形下，因接收方並非傳輸資料之控管者，故該資料控管者不負責接收資料控管者對資料保護法之合規性，惟傳輸資料之控管者應設置安全維護措施，以確保其確實代表當事人行事，例如：控管者可建立一認證程序用以確認其傳輸之個人資料類型或內容確實為當事人所欲傳輸之資料；又回應資料攜帶請求之資料控管者（原資料控管者）雖無傳輸資料前檢查和驗證資料品質之特定義務，然依據GDPR第5條第1項規定之原則，此等資料應已是正確且為最新版本之資料。值得注意的是，GDPR並未特別要求資料控制者專為提供任何未來可能發生之資料攜帶請求，而將資料

保留超出其所適用之保留期限。

(3) 控管者應與受託者共同執行特定程序，以回應資料攜帶之請求

若當事人所請求之個人資料係由資料受託者所處理，依據GDPR第28條所簽訂之契約，則必須有義務「透過適當技術性和組織性措施協助控管者，以回應當事人行使其權利之請求」，因此，資料控管者應與其資料受託者共同合作執行特定程序，以回應資料攜帶之請求，在資料控管者應與其資料受託者共同控管之情況下，據GDPR第28條所簽訂之契約應明確分配每個資料控管者間關於處理資料攜帶請求之責任。

(4) 透明化及必要範圍

「接收」資料之一方，成為當事人個人資料之新資料控管者，故必須遵守GDPR第5條中規定之原則，因此，「新的」接收資料控管者必須依據第14條規定之透明化要求，即在發送任何可攜資料傳輸請求前，清楚且直接地說明新的處理目的，接收資料控管者需負責確保其所提供之可攜資料在新的資料處理上係相關且於必要範圍內的，即被接收資料控管者接受和保留之資料應僅限於其為當事人提供服務所必需及相關之資料，若非為實現新的處理目的所必需之個人資料則應將其刪除之。但據GDPR之規定，在任何情況下，接收資料控管者都沒有義務接受和處理依資料攜帶請求傳輸之個人資料。

（三）資料可攜權與當事人之其他權利

1、 資料可攜權不會影響其他權利之行使

當個人行使其資料可攜權時，此行為並不會影響該當事人任何其他權利，即使在資料可攜權作業後，當事人仍可繼續使用資料控管者之服務並從中受益，資料可攜權並不會使傳輸資料控制者處所保留之當事人資料自其系統中自動刪除，但若當事人欲行使其刪除權（GDPR第17條規定之「被遺忘權」），傳輸資料控管者不得以資料可攜權為由，延遲或拒絕刪除。

2、 GDPR 與特定法律間之適用

若當事人之要求明確表示其所求並非在於行使GDPR中之權利，而僅係依據某特定法律行使其權利，則GDPR的資料可攜權條款將不適用於該請求；另一方面，若請求之目的係針對GDPR中所規定之可攜性，則GDPR所規定的對任何資料控管者就資料可攜權原則之一般適用仍應優先適用於該特定法律。

（四）資料可攜權之適用時機與範圍

1、 GDPR 合規性要求資料控管者須具有處理個人資料之明確法律依據。

2、 依據 GDPR 第 20 條第 1 項第 a 款，處理作業必須基於下列方式進行，方於資料可攜權之適用範圍內：

(1) 當事人之同意：依據第 6 條第 1 項第 a 款，或依據第 9 條第 2 項第 a 款，當涉及特殊類型之個人資料時，須經當事人同意。

(2) 與當事人訂立契約：依據第 6 條第 1 項第 b 款，應與當事人訂立契約。

(3) 當個人資料之處理並非基於上述兩點時，則無 GDPR 資料可攜權一般權利之適用[60]。例如，作為防止和偵查洗錢及其他金融犯罪義務之一部分所為之資料處理，金融機構並無義務回應有關此類個人資料之資料攜帶請求。而在許多情況下，由於雇主和員工之間的權力不平衡，員工的同意一般無法被視為係自由給予的，因此，通常須以個案方式來驗證是否所有適用於資料可攜權之要件皆被滿足，另須注意的是，資料可攜權僅適用於當資料處理係「透過自動化方式執行」時，因此不涵蓋大多數的書面檔案。

3、 可攜之個人資料

根據GDPR第20條第1項，在資料可攜權範圍內，資料必須是：

(1) 與當事人相關之個人資料

A. 僅有個人資料屬於資料攜帶請求之範圍內。因此，任何匿名

[60] EU, GDPR, Recital 68 and §20(3) . Article 20(3) and Recital 68 provide that data portability does not apply when the data processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, or when a data controller is exercising its public duties or complying with a legal obligation. Therefore, there is no obligation for data controllers to provide for portability in these cases.

或與當事人無關之資料皆不在此範圍內（但與其他資訊連結後可間接識別之資料，縱使非當事人之真名仍屬之）。

B. 在許多情況下，資料控管者常會需要處理到包含數個當事人個人資料之資訊，因此，資料控管者不應對「與當事人相關之個人資料」一詞採取過度限縮之解釋，例如，電話、個人間通訊等記錄可包括（在用戶帳戶歷史中）來電或去電第三方之資訊細節，雖該記錄包含相關數個當事人之個人資料，但用戶應仍能夠依資料攜帶請求取得此些記錄，因該記錄亦與該當事人相關；然而，若此些記錄隨後被傳輸至新的資料控管者，則新的資料控管者處理該資料之任何目的不得對第三方之權利和自由產生不利影響（GDPR 第 20 條第 4 項）。

(2) 由當事人提供予資料控管者之個人資料

A. 個人資料須由當事人有意識且積極主動「提供」，例如：透過網路表格提交相關資料，且觀察其活動所得之資料亦屬由當事人「提供」之資料： WP29 認為，為充分發揮此項新權利之價值，經由使用服務或設備而由當事人提供之觀察資料亦應包括，從用戶活動中觀察到的個人資料，如個人搜尋歷史、流量資料、位置資料及智慧型電錶所處理等之原始資料。

B. 惟上述資料並不包括由資料控管者創建、推論和衍生之資料，

例如：透過分析所蒐集之原始智慧型手錶紀錄資料而創建之檔案或用戶健康狀況評估之結果，此些資料通常不會被視「由當事人提供」，因此不屬於資料可攜權之範圍，鑑於資料可攜權之政策目的，「由當事人提供」一詞必須做廣義之解釋，並應排除「推論資料」及「衍生資料」，資料控管者可先排除此等資料，僅傳輸或處理包含當事人透過資料控管者所提供之技術方式而提供的其他個人資料。

（五）資料可攜權與透明化義務

GDPR第14條第3項規定「若非從當事人處獲得個人資料」，則該資訊必須在獲得後一個月之合理時間內、在與當事人進行首次溝通時、或在向第三方揭露時提供，在提供所需資訊時，資料控管者必須確保其將資料可攜權與當事人在GDPR下之其他所有權利有所區分，因此，WP29特別建議資料控管者清楚地向當事人解釋透過「存取權」及「資料可攜權」可接收之資料類型間之差異。

WP29另建議，作為接收資料控管者，應提供當事人與其將執行服務相關個人資料之性質有關之完整資訊，除了作為公正處理之基礎外，此做法亦允許當事人降低對第三方當事人個資被輸出之風險，以及任何其他非必要之複製個人資料，即使該行為並未涉及其他當事人，亦同。

（六）資料格式

GDPR第20條第1項規定，個人資料必須以「結構性、一般性和機器可讀性之格式」提供。而多樣化之組織得透過各自ICT系統之間的資料交換支援該業務程序。

第2013/37 / EU號指令前言第21點61將「機器可讀性」定義為：「使軟體應用程式可輕易識別、辨認和提取特定資料之結構化檔案格式，包括個別描述及其內部結構。以機器可讀之結構化格式編碼之檔案資料是機器可讀式資料。機器可讀格式可以是開放或專有的; 且可以是正式或非正式的標準。以限制自動處理之文件格式編碼的檔案，因不得或不易從中提取資料，所以不應視為係機器可讀格式」。

在不同產業之間會有不同的最適合之格式，例如：在金融界最適合之格式，於醫療界未必最為合適，然選擇之格式應可達到得解釋之目的，並可為當事人提供相當大程度之資料可攜權。

前言第68點[62]闡釋「當事人傳輸或接收有關其個人資料之權利不

[61] The EU glossary (http://eur-lex.europa.eu/eli-register/glossary.html) provides further clarification on expectations related to the concepts used in this guideline, such as *machine-readable, interoperability*, *open format*, *standard*, *metadata*.
歐盟術語表（http://eur-lex.europa.eu/eli-register/glossary.html）進一步闡明了與本指引中所使用概念相關之期待，例如*機器可讀性、互通性、開放格式、標準、解釋資料*。

[62] EU, GDPR, Recital, 68, ”To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. 2Data controllers should be encouraged to develop interoperable formats that enable data portability. 3That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. 4It should not apply where processing is based on a legal ground other than consent or contract. 5By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public

應加諸控管者義務以採行或維護技術上相容之處理系統。」因此，資料可攜權之目的在於產生可讓資料互通而非相容之系統。

若在特定行業或特定環境中並無一般性之使用格式，資料控管者在提供資料時應使用常用的開放性格式(例如XML，JSON，CSV，...)，並應使用合適之解釋資料，以精準地描述所交換資訊之內容含義，此解釋資料應可使資料具功能性且可再使用，但又不至致洩露商業機密之程度。因此，在選擇提供個人資料之資料格式時，資料控管者應考量該格式將如何影響或是否有可能阻礙當事人再使用資料之權利；然而，當處理額外解釋資料之唯一目的僅係可能需要或想要該額外解釋資料以回應資料攜帶請求，則此非該處理之正當依據。

WP29強烈鼓勵產業相關者和同業公會在共同合作，產生並使用一套通用且可互通之標準和格式，以符合資料可攜權之要求。

（七）可攜資料的安全維護

資料控管者應依據GDPR第5條第1項第f款之規定，確保「個人資

duties. 6It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. 7The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. 8Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. 9Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. 10Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.".

料之安全性，並使用適當技術性或組織性措施，防止包括未經授權或非法處理並防止意外遺失、破壞或損毀」。然而，將個人資料傳輸予當事人亦可能會引發某些安全疑慮：

1、 傳輸安全

(1) 採取安全必要措施及持續維護資料

資料控管者有責任採取所有必要的安全措施，不僅須確保該個人資料被安全地傳輸（透過使用端對點或資料加密）至正確目的地（透過使用強力認證措施）， 亦須繼續維護仍存留於其系統中當事人之個人資料，以及處理可能侵害該等資料之透明化程序。

(2) 降低風險措施

若當事人身份需進行驗證，則使用其他身份驗證資訊或其他身份驗證要件（如一次性手機驗證密碼）；若懷疑帳戶已遭到侵害，則立即暫停或凍結傳輸；在從資料控管者直接傳輸至另一資料控管者之情況下，則應強制使用授權驗證，例如token- based驗證。此類安全措施不得具有阻礙性，不得阻止用戶行使其權利，例如：收取額外費用。

2、 儲存安全

資料控管者可推薦適當之格式、加密工具和其他安全措施，以協助當事人維護資料儲存之安全性。

三、我國法規比較

GDPR就此一權利訂定法規後，對我國金融業、科技業、醫療業、電信業等各重要領域之衝擊皆不可謂不小，雖我國法律不受GDPR之約束，然若我國之業者符合下列條件者，仍受GDPR之約束，而GDPR之規範加重了企業責任並同時強化了當事人的權利，在此，資料可攜權便是最佳的例子之一：

（一）設立於歐盟境內之資料控管者及受託處理者。

（二）設立於歐盟境外，但對歐盟境內之當事人提供商品或服務、或監控其行為之資料控管者及受託處理者（GDPR§3[63]）；此等企業原則上應於歐盟設立代表，並受理相關事宜（GDPR§27[64]）。

目前於我國個人資料保護法中，就資料可攜權雖尚未有正式之法律規範，惟鑒於現今社會已邁入數位化、電子化環境，且個人資料之

[63] EU, GDPR, §3, "This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.".

[64] EU, GDPR, §27, "Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.
The obligation laid down in paragraph 1 of this Article shall not apply to:
processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or
a public authority or body.
The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.
The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.
The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves."

加值應用隨著科技不斷地迅速成長之下，為配合我國發展資料經濟、數位轉型之需求，與推動消費者（資料當事人）之資料權（Consumer Data Right），並為促使我國個人資料權的落實，我國亦應以有結構的、通常使用的、機器可讀的形式將資料提供與當事人，緣此，我國立法院已於民國（下同）108年4月12日立法院第9屆第7會期第9次會議中，以院總第1570號委員提案第23128號[65]「個人資料保護法」第10-1、56條條文修正草案交付一讀之程序，草案內容如下：

[65] 見 https://www.lawbank.com.tw/News/NewsContent_print.aspx?NID=159677.00，立法院委員余宛如等 20 人擬具「個人資料保護法」第 10-1、56 條條文修正草案。

立法院委員余宛如等 20 人擬具「個人資料保護法」第 10-1、56 條條文修正草案

2019-04-12

法規名稱：個人資料保護法
提案日期：中華民國 108 年 4 月 12 日
提案字號：院總第 1570 號 委員提案第 23128 號
資料來源：立法院第 9 屆第 7 會期第 9 次會議議案關係文書
提 案 人：余宛如
莊瑞雄
江永昌
劉世芳
連 署 人：蔡易餘
張廖萬堅
蔡適應
陳歐珀
蘇巧慧
邱泰源
陳靜敏
李俊俋
郭正亮
蔣絜安
蘇治芬
林靜儀
鄭運鵬
陳曼麗
郭國文
李麗芬

案　由：本院委員余宛如、莊瑞雄、江永昌、劉世芳等 20 人，現今社會已邁入數位化、電子化環境，且個人資料的加值利用價值隨科技也不停成長，配合我國發展資料經濟、數位轉型之需求，與推動消費者資料權（Consumer Data Right）之必要，並參照 GDPR 第 20 條與立法前言第 68 點，將資料可攜權明文，以促使我國個人資料權的盡一步落實，爰提出「個人資料保護法第十條之一及第五十六條條文修正草案」。是否有當？敬請公決。

說　明：為促使我國個人資料權的落實，並配合現已邁向數位化、電子化之社會環境，故明文當事人若提出閱覽或複製個資之要求，應以有結構的、通常使用的、機器可讀的形式提供與當事人，像將資料可攜權明定之。

第 10-1 條　前條所稱製給複製本，當事人得請求以電子形式交付基於當事人同意或依履行契約所必要者之資料之複製本，公務機關及非公務機關不得拒絕之。但無法執行或執行成本過高之情形不在此限。
前項所稱製給複製本，係指以有結構的、通常使用的、機器可讀的形式提供予當事人或當事人指定之第三方，且不得妨礙當事人傳輸予第三方。

第 56 條　本法施行日期，由行政院定之。但○年○月○日增訂之第十條之一自一百十四年一月一日起施行。
現行條文第十九條至第二十二條及第四十三條之刪除，自公布日施行。
前項公布日於現行條文第四十三條第二項指定之事業、團體或個人應於指定之日起六個月內辦理登記或許可之期間內者，該指定之事業、團體或個人得申請許止辦理，目的事業主管機關於許止辦理時，應退還已繳規費。已辦理完成者，亦得申請退費。
前項退費，應自繳費義務人繳納之日起，至目的事業主管機關許止辦理之日止，按退費額，依繳費之日郵政儲金之一年期定期存款利率，按日加計利息，一併退還。已辦理完成者，其退費，應自繳費義務人繳納之日起，至目的事業主管機關核准申請之日止，亦同。

四、研究發現與結論

（一）實務上資料可攜權之應用，於我國各界尚不多見，茲就少數例子合先略述如下：

1、 金管會的 OPEN BANKING[66]

過去客戶之帳戶資料、金融數據，是銀行獨自擁有的資產，而Open Banking是指銀行透過與第三方服務業者合作，以開放應用程式介面（API）共享金融數據資料，將銀行帳戶資訊之主導權還給消費者，自此，消費者有權決定是否讓其他銀行或非銀行之第三方業者存取其帳戶資料。藉由API共享金融資訊，與第三方服務業者建構應用程序及服務，並合作開發相關之應用程式（APP），為客戶提供更多財務服務。甚至透過第三方業者的協助，將金融消費者在各銀行之相關資料做整合分析，復再提供調整建議，使消費者得以將其資產做最佳的理財規劃。OPEN BANKING源自於英國和歐盟。英國在2015年開始規劃、制定並推出Open Banking的標準，且自2018年1月開始，在用戶同意之下，讓經認證的第三方機構存取帳戶數據。歐盟執委會於2015年10月所提出的「支付指令第二版（revised Payment Services Directive，PSD2）」，要求歐盟區銀行開放 （API） 授權給第三方業者使用，以提升金融支付產業的競爭力。PSD2並已於2018年1月13

[66] 參閱 https://www.moneydj.com/KMDJ/Wiki/WikiViewer.aspx?KeyID=f8ce918a-35c2-4064-bf90-f65f4f8ead4f。

日開始實施。於2019年，我國金管會針對開放銀行進行三階段開放措施，依序是商品資訊、客戶資訊及交易資訊。第一階段先公開商品資訊（不含用戶資料），如房貸利率、信用卡等金融商品；第二階段，開放客戶資訊（需客戶授權同意），包括房貸、存款、基金投資等；第三階段，開放交易資訊（可做支付等交易）[67]。

2、 國家發展委員會的數位服務個人化（MY DATA）[68]

My Data係依照個人需求提供民眾自行下載個人資料，或是透過線上服務授權方式，由民眾授權政府機關或民間業者取得其個人資料，提供民眾所需的個人化服務；為發展My Data服務，國發會研擬相關處理，例如：戶役政資料、勞健保資料、水電資料等，並處理跨機關資料交換平臺進行相關授權、身分認證、資料安全保護等作業，並帶動政府機關部門進行服務流程改造，以「民眾隨心授權、資料隨手可得」形式，取代以往民眾奔走蒐集資料才能申辦業務的無效率，使政府服務轉型為真正的「一站式」數位政府服務。

3、 健保署的健康存摺[69]

健康存摺為健保署發展之個人健康電子紀錄，民眾透過網路申辦，

[67] 見 https://udn.com/news/story/11316/3888637
[68] 見國家發展委員會就「數位服務個人化(My Data)」之簡介。
https://www.ndc.gov.tw/cp.aspx?n=8B6C9C324E6BF233&s=460617D071481C4B
[69] 見中央健康保健署中區業務組之健康存摺介紹。
http://www.nhi.gov.tw/Resource/Registration/4647_21040818%E8%AA%AA%E6%98%8E%E6%9C%83-%E5%81%A5%E5%BA%B7%E5%AD%98%E6%91%BA%E7%B0%A1%E4%BB%8B.pdf

通過身分驗證，即可隨時隨地取得個人的保險計費、繳納、就診紀錄，另外亦可查詢個人過敏、器捐意願或安寧緩和意願等醫療資料，並於就醫時提供醫師參考，縮短醫病間資訊不對等，提升醫療安全與效益。

又我國電信業目前尚未見資料可攜權應用之案例，僅近期中華電信與凱基銀行跨業合作乙案[70]，略與資料可攜權相關，茲就該案略述如下：中華電信近期與凱基銀行聯手進行的金融監理沙盒實驗，也就是透過手機號碼作為身分評等驗證，來申辦凱基銀行信用卡或貸款服務，取代傳統徵信的信用評等。此一實驗鎖定有小額貸款或信用卡需求、但沒有足夠金融信用紀錄的民眾，比如社會新鮮人、學生，要來提供一個有別於徵信機構評等的方法。團隊認為，這些民眾雖然信用紀錄不足，但應有足夠的電信使用紀錄，而電信業者原本就利用這些資料來了解客戶行為，比如消費、訂購、繳款等，進而建立電信客戶評價機制。這個機制在電信業可行，應當也可作為金融業務的徵信評等標準。但礙於法規限制，直到2018年金融沙盒法案推出後，團隊才開始申請沙盒、進行實驗。實驗的第一步，就是思考電信評等機制如何對應到金融徵信評等。在實驗室中，團隊進行了樣本資料去識別化、比對各項數據，建立信用評等模型，並產出研究分析報告，更在離開實驗室時，「銷毀所有資料」只將最終的報告帶走。不只如此，電信

[70] 見 https://www.ithome.com.tw/news/133808；JP65;，文章發表日期:2019/10/24。

評等也能辨識申請人身分，可在申請人授權之下，將電信對申請人的評等資訊，轉交給銀行業者來進行核貸、發卡。這項沙盒實驗日前已順利過關，凱基銀行更推出手機號碼辦貸款和信用卡的服務，申請人只要持有中華電信門號6個月以上、正常繳費，就能使用該服務，行動身分認證可作為創新應用，只要客戶授權自願將電信資料提供給第三方服務商，就能帶動跨產業創新服務發展的契機。除了提供對外數據分析服務，中華電信大數據處也執行了許多對內的數據分析應用。其實，早在大數據處成立前，中華電信就已擁有20多年資料倉儲經驗，資料探勘作業10多年來也未停歇過。現在，更進一步發展為資料驅動業務，在對內業務上，鎖定了客戶精準行銷、網路精準建設、門市推薦，以及營運成本節降等面向。

然上述案例僅係電信業與金融業在資料可攜權上非典型之案例，隨著科技變化及發展，未來資料可攜之便利性、可行性於應用上將更為廣泛，故將來若電信業亦發展出相關之應用，而我國尚未有資料可攜權之規定時，建議 貴會可比照金管會協助金融業者，推動OPEN BANKING等作法，以輔導之方式，推動或建立一資訊共享平台或應用程式介面（API）等自動化系統，促進業者與當事人間資料之交換，在個人資料作業系統自動化之同時，亦可強化當事人之資料自主權。

（二）未來資料可攜權納入個人資料保護法之規範後

隨著科技日新月異、蓬勃發展以及國人對個人資料之自主意識抬頭，資料可攜權在未來勢必將成為一重要之權利，我國就此權利之相關條文修正草案亦已交付一讀，已如前述，惟若將來資料可攜權納入個人資料保護法時，我國通傳業者是否有能力因應隨之而來之相關問題，不無疑問。例如，建立API之技術、發展相關數位平台之能力或是資本額是否足夠應付等等，皆是業者應慎重思考其可能面臨之困境，就我國通傳產業之現況而言，電信業因網路研發技術較純熟，資本額亦較高，故若在將來需要大量開發API等介面或功能予客戶使用時，應較無問題，惟有線電視業者因資本額較低且於網路開發等技術能力亦相對較不純熟，故若未來資料可攜權納入個人資料保護法時，建議貴會應就各業者不同之特性予以輔導及協助，以使業者符合個人資料保護法條文之規定。

參、法規判斷基準

一、目的限制與加值利用

（一）研究動機

本案目的之一在於探討個人資料加值利用的法規界線，而加值利用個人資料的最大爭議在於將有牴觸「目的限制」法律原則的風險。因此，本研究嘗試分析目的限制原則的判斷基準，並針對逾越目的之利用個人資料行為提出可能的法規因應對策。

（二）概述

「目的限制」作為先進國家個人資料保護法律的重要原則，其意涵指個人資料之蒐集、處理或利用行為均須與蒐集目的具有正當合理關聯，並且不可逾越必要範圍，即蒐集個人資料之「目的」應成為蒐集、處理與利用個人資料行為的「限制」。此原則旨在保障當事人的資訊隱私權與資訊自主權，避免個人資料在當事人合理期待的範圍之外遭取得、儲存、揭露或使用。

然而，由於我國個人資料保護法僅將利用個人資料行為區分為目的內外之利用（參第 16 條、第 20 條，並見下述），未對目的內外之判斷訂有標準，主管機關亦未對此有抽象、一般之統一基準，因此實務上業者之行為究屬目的內或外之利用，即可能存有模糊空間。尤其本案關注的個人資料加值利用行為，更需要有所依據以供業者評估須

否採取額外措施（例如將資料匿名或另取得用戶同意）以合法化其利用個人資料行為。

據此，本研究即以歐盟 GDPR 及 WP29[71]於 2013 年發布的《目的限制意見書（Opinion 03/2013 on purpose limitation，下稱 WP203 意見書）》[72]為研究對象，比較歐盟法規與評估基準，作為我國法規適用的參考。

（三）歐盟對於目的相容性的評估基準

WP203 意見書說明「目的特定」的功能及「目的相容性評估（Assessment of Compatibility）」的判斷基準。雖然 WP203 意見書之依據為歐盟《個人資料保護指令 95/46/EC》，但由於該指令與現已取代之 GDPR 關於目的限制原則（指令第 6 條第 1 項第 b 款、GDPR 第 5 條第 1 項第 b 款）之規定並無重要差異[73]，是以下對 WP203 意見書之研析涉及目的限制原則之法律條文時，本研究即以現行有效之 GDPR 條文說明。

GDPR 第 5 條第 1 項第 b 款前段規定「個人資料應依特定、明確

[71] 於歐盟 GDPR 在 2018 年生效後，WP29 的職責由歐洲個人資料保護委員會（European Data Protection Board, EDPB）取代，兩者任務均包含針對個人資料保護法律發布指引或意見。

[72] EU, WP29, Opinion 03/2013 on purpose limitation, WP203, p19.

[73] EU, Directive 95/46/EC, Article6(1)(b), “Member States shall provide that personal data must be:…(b)collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards…” / GDPR, Article5(1)(b), “Personal data shall be:…(b)collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’)…”

及正當之目的而蒐集，且不得以與該目的不相容（incompatible）的方式進一步處理[74]」。WP203 意見書認為，已蒐集之資料可能對於其他未經事前明確揭露之目的具有用處，因此也應在平衡限度內適當允許個人資料的額外利用行為。據此，條文內「禁止不相容性」的規範並未排除基於新的、不同的目的而利用個人資料，只要該利用目的、行為能通過相容性評估的檢視[75]。值得留意的是，GDPR 對於利用個人資料之行為並未區分目的內或外的利用，即僅以「是否相容」作為判斷利用行為是否合法的依據，此與我國個人資料保護法第 20 條第 1 項將利用行為區分目的內外有所不同。

WP203 意見書提出的目的相容性評估基準包含：

1、 蒐集資料的目的與利用的目的之間的關係

WP203 意見書認為[76]，此基準不應僅理解為透過文字比對最初向當事人揭露的蒐集目的與之後利用行為之間是否相容，而應包含評估利用行為是否已或多或少藉由最初揭露的蒐集目的提供暗示，或依蒐集目的而可認定是合於邏輯的利用行為，也應評估利用行為是否與蒐集目的僅有部分關聯甚至全然無關。

[74] GDPR 對於 process 的定義包含我國個人資料保護法中的蒐集、處理與利用行為。雖然 process 直譯為「處理」較符合吾人理解，但由於本研究探討焦點為我國個人資料保護法中的「利用」個人資料行為，是以下涉及 GDPR 或 WP203 意見書中的 process 一詞均譯為「利用」。

[75] EU, WP29, Opinion 03/2013 on purpose limitation, WP203, p4.

[76] EU, WP29, Opinion 03/2013 on purpose limitation, WP203, p23-24.

2、蒐集資料的背景以及當事人對於資料利用的合理期待

WP203 意見書認為[77]，此基準涉及的是評估一個合理第三人如處於當事人之情境，依照蒐集資料的背景會對利用行為有如何的期待。此基準注重控管者與當事人之間的關係之性質，所要求的不僅是審查控管者向當事人揭露的法律聲明，也包含評估在該背景及該（商業或其他）關係下，存有如何的慣例或普遍預期的行為。原則上，該利用行為越超出期待或出人意料，就越可能被認定為與蒐集目的不相容。

此外，此基準也應評估控管者與當事人之間的權力平衡。如控管者基於契約關係蒐集當事人之資料，則應審查該契約之性質及當事人與控管者間的權力平衡（例如當事人能否輕易終止契約並選擇其他提供相同服務的替代者）。又如控管者基於當事人同意而蒐集並利用個人資料，便應評估當事人作出同意的任意性，以及其同意之條款的準確性。

最後，此基準也應評估控管者的利用行為之透明性，包含控管者最初或後續向當事人揭露的資訊類型與內容。

3、資料的性質以及利用行為對於當事人的影響

WP203 意見書認為[78]，法律的目的是在對當事人提供保障，是以此基準即關注利用行為對於當事人可能產生的影響。原則上涉及資料

[77] EU, WP29, Opinion 03/2013 on purpose limitation, WP203, p24-25.
[78] EU, WP29, Opinion 03/2013 on purpose limitation, WP203, p25-26.

的敏感程度越高，相容範圍就越小。

在評估對當事人的影響時，應將有利或不利的影響均納入審查，包含第三人將來可能作成之決定或採取之行動，以及利用行為是否可能導致對特定人的區別待遇或歧視。此外還應考量當事人的精神損害，例如當事人對個人資料失去控制權或發現個人資料遭到侵害後產生的惱怒、恐懼或不安。

更廣泛來說，對當事人的影響也涉及利用資料的方式，例如該資料是否將被第三人在另一種未知後果的情境下利用、該資料是否向公眾揭露或可由多數人存取、是否利用大量個人資料或與其他資料結合（例如為了商業利益、法律執行或其他目的而對當事人進行剖析）。

原則上，對當事人的影響越不利或越不具確定性，就越難以通過相容性的評估。

4、控管者為確保公平利用並防止對當事人造成任何不適當影響所採取的安全措施

最後，WP203 意見書認為[79]，不同的相容性評估基準可互為「補償」，亦即縱使依前述三項基準評估利用行為不具相容性，仍有可能藉由額外措施調和該不相容情形。

據此，最後一項評估基準即著眼於控管者為避免當事人遭受損害

[79] EU, WP29, Opinion 03/2013 on purpose limitation, WP203, p26-27, p30-32.

所採取之措施，例如：

(1) 重新向當事人揭露目的，並視具體情形或法律規定向當事人提供選擇加入或退出的機會。

(2) 取得當事人同意，尤其在控管者有意分析或預測當事人的偏好、行為及態度，進而形成對該當事人的措施或決定時，例如為了精準行銷、行為廣告、資料仲介、定位廣告或基於追蹤行為的數位市場研究所需的追蹤及剖析之目的[80]。

(3) 將個人資料匿名或加工為聚合資訊，使其不再有識別特定人的可能（即不再受法律拘束）。

(4) 無法（完全）匿名時，適當的部分匿名或去識別（例如假名、編碼、雜湊、移除識別碼、更換唯一 ID、引進「噪音」及其他技術），並單獨保存並加密可將部分匿名資料與原始資料相關聯的資料。

(5) 以契約控管受託利用資料的第三方之義務。

(6) 在可受控制的場域及網路中提供資料存取。

(7) 其他額外安全措施，例如加密。

（四）以歐盟評估基準適用案例

如以前揭歐盟評估目的相容性的 4 項基準操作，下列案例將得出如下結論：

[80] EU, WP29, Opinion 03/2013 on purpose limitation, WP203, p26-27, p46.

1、 通傳業者於帳單或信封上配合政府機關刊載政令宣導，或於帳單信封內夾寄其他業者之廣告資訊後寄送予用戶

就「蒐集資料的目的與利用的目的之間的關係」而言，通傳業者為履行契約之目的蒐集用戶的地址或電子郵件信箱，但如寄送資訊之內容與該業者本身業務完全無關，其利用行為恐即難通過相容性評估。我國法務部亦認為屬於目的外利用個人資料之行為[81]。

2、 通傳業者提供用戶資料予第三方

就「蒐集資料的目的與利用的目的之間的關係」而言，通傳業者基於履行契約、消費者管理、客戶服務等目的取得用戶之資料，此與將資料提供給與前述目的無關之第三方的行為應無正當關聯；在「蒐集資料的背景以及當事人對於資料利用的合理期待」方面亦應超出用戶的合理期待；且從「資料的性質以及利用行為對於當事人的影響」來看亦可能因對第三人提供用戶資料，致使用戶增加資料安全性或資

[81] 法務部，107 年 7 月 3 日，法律字第 10703507550 號書函，「……非公務機關原則上應於蒐集之特定目的必要範圍內利用個人資料，如使用基於契約或類似契約關係下取得之個人資料，對當事人進行行銷，應合乎社會通念下當事人對隱私權之合理期待，故『行銷行為內容』與『契約或類似契約』二者間，應有正當合理關聯，始符合上述規定特定目的內利用範疇……核其內容屬不特定多數人可以分享之利益，因此貴公司於帳單內或信封上配合前揭計畫刊載政令宣導雖非屬原蒐集客戶資料之特定目的內利用，然可認符合本法第 20 條第 1 項但書第 2 款所稱『增進公共利益』，而屬得為特定目的外利用之情形」。法務部，102 年 7 月 5 日，法律字第 10203507340 號函，「……非公務機關使用基於契約或類似契約關係下取得之個人資料，對該個人當事人進行行銷，應合乎社會通念下當事人對隱私權之合理期待，故『行銷行為內容』與『契約或類似契約』二者間，應有正當合理之關聯，始符合本法第 20 條第 1 項本文規定特定目的內利用之範疇，而無需再得『當事人書面同意』（同條項但書第 5 款）。如行銷與當事人契約或類似契約內容無涉之商品或服務資訊，則除符合本法第 20 條第 1 項但書第 1 款至第 5 款事由外（例如：為增進公共利益或免除當事人生命、身體、自由、財產上之危險等事由），應依同條項第 6 款規定經當事人書面同意者（同意方式請依個人資料保護法第 7 條第 2 項規定），始得為之……」。

訊控制權的風險，應無法通過相容性評估。我國法務部亦認為屬於目的外利用個人資料之行為[82]。

3、 通傳業者對潛在用戶舉辦活動後，寄送活動參加獎品（例如線上購物折扣券）至參加者的電子郵件信箱，並寄送其他行銷資訊至參加者的電子郵件信箱，亦利用參加者留下的資料進行分析

業者寄送活動參加獎品之行為，就「蒐集資料的目的與利用的目的之間的關係」而言應可認為該行為是以雙方曾有的契約關係為依據；在「蒐集資料的背景以及當事人對於資料利用的合理期待」方面亦應不致超出參加者的期待而使其感到意外；且從「資料的性質以及利用行為對於當事人的影響」來看應不會造成當事人的其他侵害，因此應具備相容性。

但業者如亦向參加者於活動結束後寄送其他行銷資訊，由於業者與參加者間除該次活動外另無其他契約或類似契約之關係（參加者或甚至期待業者於活動結束後，因蒐集之目的消失而依個人資料保護法第 11 條第 3 項規定主動刪除資料），且事後收到業者的行銷資訊可能超出參加者的預期，甚至將因頻繁接受行銷而感到侵擾，因此應認為無法與蒐集目的相容。我國法務部亦認為屬於目的外利用個人資料之

[82] 法務部，106 年 7 月 25 日，法律字第 10603510340 號函，「……電信公司如基於『契約關係』（代號：069） 或「經營電信業務與電信加值網路業務」（代號：133） 之特定目的為客戶個人資料之蒐集及處理，依個人資料保護法第 20 條第 1 項規定，原則上應於蒐集之特定目的必要範圍內利該等個人資料。故○○電信公司若將其客戶之個人資料提供予貴部辦理各項交通統計調查，則屬特定目的外利用……」。

行為[83]。

至於業者分析參加者資料之行為，亦由於業者與參加者間除該次活動外另無其他契約或類似契約之關係，參加者對於業者於活動結束後仍保存資料更進而作為分析之用可能感到意外，因此該行為恐無法通過相容性評估。我國法務部亦認為屬於目的外利用之行為[84]。

4、 通傳業者對某服務之既有用戶行銷該業者之商品或服務

就「蒐集資料的目的與利用的目的之間的關係」而言，由於該用戶與業者間存有持續生效的契約關係（此於前述案例(3)有所不同），業者在此關係下透過事前揭露而讓用戶知悉將接收行銷訊息，應不致與蒐集目的不相容；在「蒐集資料的背景以及當事人對於資料利用的合理期待」方面亦應不超出用戶的合理期待，且從「資料的性質以及利用行為對於當事人的影響」來看應不會造成當事人的其他侵害，因而具備相容性。

即便業者向某服務之用戶行銷該業者其他服務之資訊(例如電信業者向行動通信契約用戶寄發該電信業者經營之市話或固網服務行

[83] 法務部，106 年 6 月 15 日，法律字第 10603503880 號函，「……如將基於契約關係所蒐集之個人資料用於寄送講座贈品之目的使用，因該利用行為未逾越原蒐集之特定目的範圍，是未違反個人資料保護法第 20 條規定。惟若欲將所蒐集個人資料為特定目的外利用（例如：作為其他行銷之用）……」。

[84] 法務部，102 年 8 月 8 日，法律字第 10203508900 號書函，「……旅館業如基於住宿『契約或類似契約關係』所蒐集之線上訂房與散客住宿個人資料（本法第 19 條第 1 項第 2 款參照），應於蒐集之特定目的必要範圍內為利用；如使用於非原蒐集之特定目的之行銷或分析等特定目的外之利用，則應有本法第 20 條第 1 項但書各款情形之一，始得為之（如第 6 款『經當事人書面同意』……）」。

銷廣告），本研究認為也不致超出用戶的合理期待而構成侵擾，亦應具備相容性。

5、 通傳業者分析所保有的用戶資料，產出匿名化的分析結果，作為內部商業決策的參考，或將該結果提供第三方

業者在持續生效的契約關係下分析所保有的用戶資料，且分析產出之結果已達匿名化程度，此行為透過事前的明確揭露應不出於用戶意料之外，且對用戶不會造成其他侵害，應具備相容性；而因分析產出之結果如果已達匿名化程度，將該結果提供第三方之行為即已不受個人資料保護法的拘束。

6、 通傳業者為了例如精準行銷、行為廣告、定位廣告所需的追蹤及剖析（貼標）之目的，利用用戶之資料（例如帳單資訊、位置資訊、網頁瀏覽資訊、收視紀錄等）分析或預測用戶的偏好、行為及態度，進而形成對該用戶的措施或決定（例如決定向該用戶行銷何種商品或服務）

由於業者利用線上追蹤技術（例如 cookie、web beacon 或其他類似技術）蒐集用戶的網路行為，對當事人而言通常超出其預期；且業者利用大量各方資料對用戶剖析、貼標以分析其偏好或預測其行為，將使業者對用戶產生當事人無法知悉的「評價」，當事人的資訊自主權恐有減損，甚至會有當事人所不知的「資料不正確」或「歧視」問

題，也可能因此損害當事人的自由（例如用戶不願因其瀏覽之網頁或出入之場所而被業者劃歸為某種類型，因而自我限制行為自由），因此恐難通過相容性評估。

（五）與我國法規比較

如前所述，歐盟 GDPR 以利用行為是否與蒐集目的相容作為評估利用行為合法性的基準，相較之下，我國個人資料保護法第 20 條第 1 項將利用個人資料之行為區分為「目的內」與「目的外」之利用[85]，再對目的外利用行為訂定數項例外合法事由，此規範與前揭 GDPR 的「禁止不相容」有所差異，且從法條文義解釋亦難導出我國法律允許以額外措施（前揭 WP203 意見書提出的相容性評估基準第 4 項）調和目的外利用合法性的意旨，應無法直接援引前揭 WP203 意見書提出的相容性評估基準作為我國判斷目的內外利用個人資料之標準。

然而前揭評估基準應仍有對應我國法律的參考研究價值。依前 3 項基準即「蒐集資料的目的與利用的目的之間的關係」、「蒐集資料的背景以及當事人對於資料利用的合理期待」、「資料的性質以及利用行為對於當事人的影響」可知，**在業者以個人資料保護法第 19 條第 1**

[85] 我國，個人資料保護法，第 20 條第 1 項：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為增進公共利益所必要。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、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經蒐集者依其揭露方式無從識別特定之當事人。六、經當事人同意。七、有利於當事人權益」。

項第 2 款「與當事人有契約或類似契約之關係，且已採取適當之安全措施」作為蒐集當事人資料的法律依據時，利用行為必須與「該業者基於履行該契約之目的」此背景具備正當合理關聯，且不應使一般理性之當事人感到意外，更不可對當事人增加額外風險，否則應認定為目的外之利用。

第 4 項評估基準「控管者為確保公平利用並防止對當事人造成任何不適當影響所採取的安全措施」中的「取得當事人同意」與「匿名化資料」則與我國法規環境下的目的外利用合法事由相呼應，前者為個人資料保護法第 20 條第 1 項但書第 6 款的例外事由，後者按時為個人資料保護法主管機關的法務部（現主管機關為國家發展委員會）之函釋見解[86]，亦認將不受個人資料保護法之拘束。

（六）研究發現與結論

綜上所述，本研究將通傳業者利用用戶個人資料之行為區分為兩種情境：

1、將用戶資料提供予第三方

除非是為履行雙方契約所不可或缺，否則該行為因與契約無關，亦逾越用戶之合理期待，且可能造成用戶的資訊安全或資訊控制的風

[86] 法務部，103 年 11 月 17 日，法律字第 10303513040 號函，「……如將公務機關保有的個人資料處理技術去識別化而呈現方式已無從直接或間接識別特定個人，即非屬個人資料，自非個人資料保護法之適用範圍……」。

險，應認定為目的外利用行為。

本案關注的資料加值利用可能包含此類行為，此時業者應可以「匿名化資料」方式，使該資料不再屬於個人資料，或另行以適當方式取得用戶之同意，作為合法利用之依據。

2、 未將用戶資料提供予第三方

此利用情境可再細分為「未與用戶互動」及「與用戶互動」兩種子情境：

(1) 未與用戶互動

常見實例即為利用用戶之個人資料作為分析之用，且該分析產出之結果已達匿名程度，無法識別特定之用戶，而業者以該結果作為內部改善商品或服務等商業決策之參考，或將該結果提供（通常應為出售）予第三人。由於該結果已達匿名程度，對該結果之利用行為即無需以個人資料保護法為管制。即此時用戶（可識別個人）資料因未提供予第三人，並未增加用戶的額外資料安全或未獲授權利用之風險；且該行為不需用戶參與（例如對用戶行銷），因此亦未增加用戶遭受侵擾之機會。

(2) 與用戶互動

常見實例為利用用戶資料與用戶聯繫或向其行銷，以及剖析用戶資料後預測其偏好（貼標），進而對該當事人精準行銷。

如業者是為與雙方契約履行相關之目的而與用戶聯繫(例如客戶服務、障礙通知、寄送帳單、帳款催收等),此行為與契約履行具有正當關聯,屬於目的內利用應無疑問。若業者與用戶聯繫或行銷之內容與雙方契約之履行無關時(例如傳遞政令宣導資訊或寄送第三方業者的廣告),該行為即構成目的外利用。

在行銷方面,如業者向當事人行銷與該契約提供之服務有關的商業資訊(例如當事人申辦行動上網服務,業者向其推薦新推出的行動上網升級方案;或業者分析當事人近期的使用情形後,向其精準推薦更適合的費率方案),並未造成當事人額外風險,應屬目的內利用個人資料之行為;即便業者向當事人行銷該業者的其他服務時,本研究認為亦未造成當事人不可預期的侵擾,也應屬於目的內利用個人資料。

惟如業者為了例如精準行銷、行為廣告、定位廣告所需的追蹤及剖析(貼標)之目的,利用用戶之資料(例如帳單資訊、位置資訊、網頁瀏覽資訊、收視紀錄等)分析或預測用戶的偏好、行為及態度,進而形成對該用戶的措施或決定(例如決定向該用戶行銷何種商品或服務)時,本研究認為恐超出用戶的合理期待,甚至造成用戶權利與自由的減損,應認為屬於目的外利用。

二、歐盟「行政罰鍰」指引

（一）研究動機

隨著全球化加速擴張個人資料蒐集、控管、流通、處理之規模，使過去第 95/46/EC 號指令對於個人資料保護已然不敷使用，是以，歐洲議會與歐盟理事會於 2016 年 4 月 27 日通過歐盟規則第 2016/679 號一般資料保護規則（General Data Protection Regulation, GDPR），取代過去歐盟於 1995 年 10 月 24 日制訂並施行逾 20 年之第 95/46/EC 號指令[87]。GDPR 被視為高規格的個人資料保護規則，在違反行為的處罰上，GDPR 提供了制裁手段之選擇、鉅額行政罰鍰以及制裁同一性等規則，此規則不僅對歐盟各會員國有影響力，世界各國對於此規則亦有高度的關注，而我國立處於世界地球村的要角，了解 GDPR 的應用與處罰手段更是必要，本研究希望藉由了解 GDPR 在行政罰鍰上之應用，作為我國現行的制度之參考。

（二）概述

GDPR 乃一體適用於歐盟全體會員國，各會員國無需再制訂法規予以內國法化，此提升個人資料保護的高度與一致性，排除個人資料在歐盟間流通之阻礙，可改善過去歐盟各會員國依據第 95/46/EC 號

[87] 一般通稱為歐盟個人資料保護指令（Data Protection Directive，全稱為 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data），需透過各會員國制訂內國法將此個人資料保護指令內國法化。

指令執行時，對於個人資料保護程度的差異。此外，GDPR 更確立了鉅額之法定裁罰及計算基準，透過對違反規則行為之嚇阻效果進而建構有力的保護框架。

以下將引用 GDPR 內容及相關指引介紹 GDPR 對違反規則行為之裁處，特別著重第 83 條所列，分別以裁處機關、制裁與保護、裁處行政罰鍰之一般要件等內容作逐一說明，並援引我國現行法規制度進行比較，最後再對我國未來個人資料保護走向提出構想供研究參考。

（三）實施矯正措施之主要原則

1、 裁處機關

(1) 監管機關之設立

根據 GDPR 第 51 條所定，為保護當事人有關之個人資料處理之基本權與自由，及促進歐盟內個人資料之自由流動，歐盟各會員國應設立至少一個獨立公務機關[88]，負責 GDPR 之適用與監控，該獨立公務機關又稱為監管機關（supervisory authority），而各監管機關應致力 GDPR 於歐盟全體之一致適用[89]。

[88] EU, GDPR, §51 (1), “each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (‘supervisory authority’).”

[89] EU, GDPR, §51 (2), “each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.”

(2) 監管機關之職責

根據 GDPR 第 57 條第 1 項 g 款所定，各監管機關除監控及執行 GDPR 之適用外，亦須與其他監管機關合作，包括分享資訊及互助，以確保 GDPR 適用上之實質一致性[90]；因此 GDPR 雖然在第 58 條中賦予各監管機關對控管者與受託者有調查權及糾正權，然為符合實質一致性之要求，縱使各監管機關可依據 GDPR 第 58 條第 2 項第 b-j 款之規定，對控管者或受託者不合規之情形發布警告、告誡、遵循要求等矯正措施，各監管機關為前揭矯正措施時仍應有「同等之制裁」之適用，甚至在行政罰鍰適用範圍上，縱使某些歐盟會員國的法律制度不允許以 GDPR 所規定之行政罰鍰為處罰，惟當此些成員國適用各該國法規時，仍需與監管機關得處以之行政罰鍰效果相當，避免有制裁上的差異[91]。

2、 制裁與保護

(1) 同等程度之保護

由於 GDPR 可直接適用於歐盟各成員國，因此相較過去第 95/46/EC 號指令，GDPR 要求各會員國在個人資料保護及流通上有更大程度的一致性，亦即所有會員國對個人資料的保護應有「同等程度

[90] EU, GDPR, §57 (1), (g), cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation.
[91] EU, WP29, Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679 At 5.

之保護」。而所謂同等程度之保護係指需有「同等程度之權力以監控和確保個人資料保護規則之遵守，以及成員國對違反規則行為有同等程度之制裁」[92]。

(2) 同等程度之制裁

各監管機關雖然完全獨立於國家政府、控管者或受託者，然而透過 GDPR 的要求，在跨境案件上各監管機關仍必須相互合作，以確保 GDPR 適用和執法之一致性。此外，各監管機關雖然依第 58 條第 2 項規定得選擇矯正措施予以執行，但仍應避免在類似案件中選擇不同之矯正措施，以確保執法之一致性[93]。

3、 裁處行政罰鍰之一般要件

(1) 有效、適當且具勸阻性

除告誡、警告、禁止等矯正措施外，GDPR 亦設有行政罰鍰之規定，行政罰鍰與其他矯正措施相同，第 83 條第 1 項即開宗明義要求各監管機關應確保行政罰鍰之制裁在個案中係有效、適當且具勸阻性[94]，因此各監管機關必須評估每個案件的事實，考慮選擇之矯正措施所追求之目標，例如重新要求對規則之遵守，或欲處罰違反規則之行

[92] Id. At 6, “equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.”
[93] Id. At 5.
[94] EU, GDPR, §83 (1), “Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.”

為（或兩者均追求之）[95]。

(2) 個案評估

GDPR 第 83 條第 2 項列有 11 款提供監管機關對違反規則是否應處以罰鍰及罰鍰金額時之考量標準，主要內容逐條說明如下：

A. 違反規則行為之性質、嚴重程度及持續期間，並考量到資料處理之範圍或目的，以及受影響之當事人人數及其受損程度[96]

GDPR 將違反規則之行政罰鍰標準臚列於第 83 條第 4 項至第 6 項，藉由「最高處以 1 千萬歐元之行政罰鍰金額，或如為企業者，最高達前一會計年度全球年度總營業額 2%，並以較高者為準」及「最高處以 2 千萬歐元之行政罰鍰金額，或如為企業者，最高達前一會計年度全球年度總營業額 4%，並以較高者為準」之分層系統[97]供監管機關作為酌定違反規則行為時得處之最高罰鍰金額；而 GDPR 亦藉由前揭規則內容而揭示違反部分條款的嚴重程度顯大於其他條款，因此監管機關在依據第 83 條第 2 項

[95] WP29, supra note 5, at 6.
[96] EU, GDPR, §83 (2) (a) , "The nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected, and the level of damage suffered by them."
[97] EU, GDPR, §83 (4), "infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. Article 83 (5), infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. Article 83 (6), non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher."

評估案件事實後，可對該違反規則行為選擇適當之矯正措施，若行政罰鍰被選擇為最適當之矯正措施時，即可以分層系統所示之行政罰鍰標準論處[98]。惟仍須注意在構成「輕微違反」時，此類違反規則行為雖可構成違反同條第 4 項或第 5 項中所列之一項或多項規定，然而監管機關仍可以根據同條第 2 項的評估標準，在案件的具體情狀下，以告誡取代罰鍰（非義務性，僅為可能之選擇）。此外，第 83 條第 6 項「最高金額 2 千萬歐元或企業高達前一會計年度全球總營業額之 4%」之案件可能是監管機關已依第 58 條第 2 項之規定發布命令，而控管者或受託者未能遵守該命令[99]。

控管者或受託者違反規則行為嚴重程度則係藉由該違反行為之性質，以及「考量到資料處理之範圍或目的，以及受影響之當事人人數及其受損程度」等為判斷依據[100]；惟監管機關在評估時仍須秉持有效、符合比例原則和具勸阻性等原則，在發現有違

98 WP29, supra note 5, at 9.

99 需考慮到歐盟各會員國的國家程序法，依各國法律決定命令如何發布、如何被通知、命令從何時起生效、是否存在合規性之寬限期等，亦應注意上訴對命令的可執行性，詳參 Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679（關於第 2016/679 號規則中的行政罰鍰適用和制定之指引）註釋 9：Application of article 83(6) necessarily must take into account national law on procedure. National law determines how an order is issued, how it is notified, from which point it takes effect, whether there is a grace period to work on compliance. Notably, the effect of an appeal on the enforceability of an order should be taken into account.

100 EU, WP29, supra note 5, at 10, “the scope, purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them” Article 29 Working Party, supra note 5, at 10.

反第 8 條和第 12 條之行為時，仍可處以第 83 條第 5 項規定之高額罰鍰，以對應最嚴重之違反規則行為[101]。

另外，資料處理之範圍及目的亦屬監管機關在評估擇處裁罰之重點，例如可透過受侵害之當事人數量以茲辨別該違反規則行為係獨立事件或系統性侵害、資料被處理的目的是否具有正當性、若當事人遭受損害時，監管機關在選擇矯正措施時即應考量其受損害之程度，縱使監管機關本身無權對當事人所遭受之損害給予具體的賠償，然該行政罰鍰的課處並不取決監管機關在侵害和實質損害間建立因果關係之能力[102]。

至於持續期間則視資料控管者是否屬故意行為、是否未採取適當之預防措施，或無能力實施所需之技術性和組織性措施[103]等判斷之。

B. 違規之故意或過失[104]

通常在認定上，故意行為相較過失行為更為嚴重，因此更有可能被處以行政罰鍰，其可能之情狀包含來自控管者最高管理層級明確授權之非法處理，或儘管個資保護長已提出建議或根本無視現有政策，例如意圖使市場上的競爭對手失去信譽而取得及處

[101] Id. At 10.
[102] Id. At 11.
[103] GDPR 第 23 條及第 32 條將實施個人資料保護之技術性及組織性措施，視為控管者及受託處理者之責任。
[104] EU, GDPR, §83 (2) (b), “the intentional or negligent character of the infringement.”

理競爭對手之員工資料。其他可能故意情狀包含為達成某種誤導性目標而修改個人資料、漠視當事人關於如何使用其資料之主觀意識即販售個人資料等[105]。

至於過失情狀，如未能了解或遵守現有政策、人為錯誤、未能檢查公布資訊中之個人資料、未能及時實施技術性更新、未能採行政策（非單純的不加以應用）等。此外，故意與過失間尚有些灰色地帶，因此監管機關在判斷違反規則行為之意圖時，務必要對個案進行更廣泛之調查，以確認案件事實，並確保充分考量到每個案件的所有具體情況[106]。

C. 控管者或受託者為減輕當事人所遭受之損害而採取之任何行動[107]

過去在第 95/46/EC 號指令施行時，當資料控管者或受託者已承認有違反規則行為，並透過改正或限制等補救而承擔責任時，例如發現誤將個人資料與其他延伸之控管者或受託者分享時即盡速聯繫，或採取相應之行動以阻止侵害之繼續或擴大至相當程度等，則監管上給予適度的彈性是必要的；而本條款亦屬在違反規則行為發生後，監管機關得將資料控管者和受託者是否已盡其所能減輕該侵害行為對相關當事人之損害，納入在選擇矯正措施

105 -EU, WP29, supra note 5, at 12.
106 Id. at 13.
107 EU, GDPR, §83 (2) (c), "…any action taken by the controller or processor to mitigate the damage suffered by data subjects."

以及計算特定案件中之罰鍰金額之考量[108]。

D. 控管者或受託者之責任程度，需考量到其依據第 25 條和第 32 條所執行之技術性和組織性措施[109]

資料控管者和受託者有義務實施技術性和組織性措施，以確保適合風險之安全層級、執行資料保護影響評估、並減輕處理個人資料對當事人權利和自由所造成之風險。本條款的制訂，使 GDPR 在資料保護上，與第 95/46/EC 號指令相較，前者引進了更高層級之資料控管者責任，亦即控管者必須行「方法式之義務」[110]，提出適宜之技術性及組織性措施，以落實對個人資料適當程度之安全維護。

E. 控管者或受託者過去任何相關之違反規則行為[111]

如前提及，GDPR 要求監管機關對個案的違反規則行為評估時，務必要對個案進行更廣泛之調查，故控管者或受託者過去曾有任何違反規則行為，縱使該行為與監管機關現在正調查之案件無關，惟其無視資料保護規則或認知不足等任何違反規則之行為仍可被監管機關納入評估，因此監管機關應評估控管者或受託者過去是否曾犯過相同之「違反行為」，及控管者或受託者是否以

108 EU, WP29, supra note 5, at 13.
109 EU, GDPR, §83 (2) (d), "the degree of responsibility of the controller or processor taking into account technical and organizational measures implemented by them pursuant to Articles 25 and 32."
110 EU, WP29, supra note 5, at 13.
111 EU, GDPR, §83 (2) (e), "any relevant previous infringements by the controller or processor."

相同之「方式」違反了本規則，例如對組織中現有慣例之認知不足，或由於不適當之風險評估而未能即時回應當事人要求等[112]。

F. 與監管機關之配合程度，以改正違反行為並減輕違反行為可能產生之不利影響[113]

當監管機關決定是否對違反規則行為處以行政罰鍰並計算罰鍰金額時，得將控管者或受託者對監管機關已確認之違反規則行為行改正之程度列入考量，惟仍應有比例原則之適用[114]。

G. 受違反規則行為影響之個人資料類型[115]

在受影響之個人資料類型上，較關鍵的判斷係該資料是否屬第 9 條及第 10 條之特殊類型資料、是否可以直接或間接識別，是否涉及擴散會對個人造成直接傷害或痛苦之資料、該個人資料是否在沒有技術性保護之情況下可直接使用，或者是否已加密等均屬之[116]。

H. 監管機關得知違反規則行為之方式，尤其係控管者或受託者是否就該違反行為進行通知，以及通知之程度為何[117]

112 EU, WP29, supra note 5, at 14.
113 EU, GDPR, §83 (2) (f), "the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement"
114 WP29, supra note 5, at 14.
115 EU, GDPR, §83 (2) (g), "the categories of personal data affected by the infringement."
116 EU, WP29, supra note 5, at 14-15.
117 EU, GDPR, §83 (2) (h), "the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement."

根據 GDPR 所示，當個人資料受侵害時，控管者有義務向監管機關通報，因此控管者縱使行此項義務，仍不得將其對義務之遵守解釋為違反規則行為之減輕因素；惟若控管者或受託者因不注意而未能通知，或因沒有充分評估違反行為之程度而導致未能就違反行為之所有細節進行通知時，監管機關可考量處以較嚴厲之懲罰，亦即該違反行為不太可能被歸類為「輕微違反」[118]。

I. 先前已就有關同一主題事件，向相關控管者或受託者發布命令，要求其遵守第 58 條第 2 項所述之措施[119]

監管機關為控管先前違反行為之合規性，可能與個資保護長有大量聯繫，因此，監管機關將考量先前之聯繫狀況。此評估標準之目的僅為提醒監管機關考量其先前已向同一控管者或受託者「基於同一主題事件」所實施之措施[120]。

J. 遵守依據第 40 條認可之行為守則或依據第 42 條認可之認證機制[121]

依據 GDPR 第 24 條第 3 項、第 28 條第 5 項或第 32 條第 3 項，控管者或受託者可使用經認可之行為守則作為證明其合規性

[118] EU, WP29, supra note 5, at 15.
[119] EU, GDPR, §83 (2) (i), where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures
[120] EU, WP29, supra note 5, at 15.
[121] EU, GDPR, §83 (2) (j), "adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42."

之方式。當控管者或受託者遵守經認可之行為守則時，監管機關或許可信賴負責管理守則之守則社群對其成員採取適當之行動，例如透過對行為守則本身之監督和執行計畫。因此，監管機關可能會認為此些措施於該特定情況下是屬有效、符合比例原則或具勸阻性的，而無需由監管機關本身施以額外之矯正措施[122]。

K. 適用於案件情狀之任何其他加重或減輕因素，例如直接或間接從違反行為中獲得或避免損失之經濟利益[123]

此條款直接說明可將其他因素納入考量以決定因違反同條第 4 至 6 項而處以行政罰鍰之適當性，尤其控管者因違反行為而獲利之事實即可作為處以罰鍰之決定要素[124]。

(3) 裁處金額

參照前揭之討論，GDPR 第 83 條第 2 項提供監管機關最有效用之標準予以辨別案件事實，以決定除第 58 條所規定之其他措施外，是否應對控管者或受託者之違反規則行為處以適當之行政罰鍰；惟 GDPR 所列之行政罰鍰並未對特定違反規則行為給予具體之「價格標籤」，僅有最高行政罰鍰上限[125]，故監管機關仍應評估出最有效、符合比例原則和具勸阻性之罰鍰金額，以回應違反規則行為。

---

122 EU, WP29, supra note 5, at 15.
123 EU, GDPR, §83 (2) (k), "any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement."
124 EU, WP29, supra note 5, at 16.
125 EU, WP29, supra note 5, at 9.

此外，GDPR 亦建議各監管機關依第 83 條之規定，考量每一個案之所有情況後行一次性評估，即在第一階段評估中得出之結論可在關於罰鍰金額的第二階段中援用，從而避免使用相同之標準評估二次；且縱僅透過罰鍰實現制裁行為亦無不可，並非總是需要透過使用一個矯正措施來補充另一矯正措施，而監管機關之作用即係透過矯正措施以恢復合規性[126]。

至於，一致性行政罰鍰是 GDPR 施行後持續發展之目標，透過案件處理研討會或其他活動進行定期交流、對來自次國家、國家和跨境層級之案例進行比較等，各監管機關間可相互合作，共同努力，以實現一致性[127]。而歐盟個資保護工作小組於「關於第 2016/679 號規則中的行政罰鍰適用和制定之指引」即指出，建議未來成立一個隸屬於 EDPB 相關部門之永久性小組以持續支援一致性行政罰鍰之任務[128]。

（四）與我國現行法之差異

我國個人資料保護法（下稱個人資料保護法）的制定，係將過去國際上對個人資料保護的「目的限制」原則納入立法精神中，要求公務機關及非公務機關於蒐集個資應有「特定目的」，其等利用個人資料行為應與蒐集之特定目的相符，並導入告知義務、當事人同意、當事人權利、資料保存、蒐集者責任等相關規範，明確強化了個人資料

126 Id. At 17.
127 Id.
128 Id.

蒐集、處理與利用之保護，使個人資料的使用上相較於傳統受到更多的約束，以下將從對控管者的責任要求、行政罰鍰的標準、其他裁罰措施等比較 GDPR 所揭示之原則為差異。

1、 責任要求：目標式義務與方法式義務

自前揭 GDPR 第 83 條第 2 項 d 款內容，可知道 GDPR 在要求資料控管者或受託者於個人資料蒐集、處理及處理上，必須實踐保護程度之技術性措施及組織性措施等責任，此種所謂的「方法式之義務」，大大的改變了過去僅以「目標式之義務」（如目的限制原則）為主之思維，亦即 GDPR 更進一步要求控管者或受託者必須主動對個人資料保護進行相當措施之規劃[129]，例如在處理個人資料可能導致自然人之權利及自由的高度風險時，控管者應於茲料處理前，實行該處理對於個人資料保護之影響評估[130]，或是在一定條件下設置資料保護長（DPO）[131]，以因應大規模處理特種個人資料；因此，GDPR 的施行已不如過去僅要求控管者或受託者在個人資料蒐集、利用、處理時被

[129] Id. At 13.
[130] EU, GDPR, §35 (1), "where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the 72 protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."
[131] EU, GDPR, §37 (1), "The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10."

動的被檢視蒐集個資是否合乎特殊目的，或其利用行為與目的具有合理之關聯性等目的性限制。

而我國個人資料保護法對於資料蒐集者的責任主要區分為安全維護義務及事故通知義務，以個人資料保護法第 27 條為例，該條文規定非公務機關保有個人資料檔案者，應採取適當之安全維護措施，以確保個人資料不受到侵害，而所謂安全維護措施，則根據個人資料保護法施行細則第 12 條第 2 項規定，係認公務機關或非公務機關在符合比例原則的前提下採取包含風險評估、建立管理秩序、安全稽核、記錄保存等作為[132]；至於事故通知義務則係依個人資料保護法第 12 條之規定，公務機關或非公務機關違反個人資料保護法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。是以，我國個人資料保護法對於蒐集者的責任，並未要求公務機關或非公務機關設立資料保護長行大規模特種個資處理，仍是遵循著制定個人資料保護法時引進之「目的限制」原則為框架，透過合目的性之規範、行為與目的間具有合理之關聯性等，行被動式的個人資料保護。

此外，我國現行之電信法或資通安全管理法雖就通信秘密保護、

[132] 個人資料保護法施行細則第 12 條雖就個人資料保護法所稱之安全維護措施，說明該安全措施係指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施，並例示該等措施得包括之事項，惟個人資料保護法及施行細則對大規模的資料處理、特殊資料的處理上，並沒有特別對使用方式進行區分，亦未設置資料保護長主責執行。

資訊安全維護有相關之立法，卻未見此揭法律條文對資料控管者及受託者於相關個人資料蒐集、處理或利用時，有顯著的個資保護措施之要求，對於個人資料的處理保護尚屬不足。

2、 行政罰鍰界線與裁罰標準

根據 GDPR 第 83 條第 4 項至第 6 項，違反 GDPR 規範者，最高得處以 2,000 萬歐元或其年度總營收 4%之罰鍰，適用對象限於企業，未針對自然人或公務機關之違反行為制定處罰規範，而罰鍰的界線與標準也因為 GDPR 僅提出罰鍰適用之範圍，未明確劃分何違反行為應處以多金額的行政罰鍰，現階段僅能透過各會員國間遵照「關於第 2016/679 號規則中的行政罰鍰適用和制定之指引」所示，透過跨境間之交流、各國間相互合作，甚至倡議成立一個隸屬於 EDPB 相關部門之永久性小組以支援 GDPR 倡導之一致性、同等性之裁罰[133]。

我國國家通訊傳播委員會就通訊傳播事業違反個人資料保護法事件，在 104 年 6 月 2 日訂有「國家通訊傳播委員會裁處通訊傳播事業違反個人資料保護法罰鍰案件處理要點」(下稱罰鍰處理要點)，此要點係依個人資料保護法第 47 條至第 50 條，所定提供主管機關對通訊傳播事業違反個人資料保護法時相應之處置，依其情節輕重，得按次處「新臺幣 2 萬元以上，新臺幣 20 萬元以下」，或「新臺幣 5 萬元

133 EU, WP29, supra note 42.

以上，新臺幣 50 萬元以下」之罰鍰。

前揭罰鍰處理要點之附件「國家通訊傳播委員會裁處通訊傳播事業違反個人資料保護法罰鍰案件違法行為評量表」（下稱違法行為評量表），以違法情節之分級說明給予主管機關對論處通傳事業違反個人資料保護法規定時之評分基準，併與同部罰鍰要點之他附件「國家通訊傳播委員會裁處通訊傳播事業違反個人資料保護法罰鍰案件額度參考表」（下稱罰鍰額度參考表），係針對評分內容進行等級劃分予以確定罰鍰額度，此等評分基準與裁罰金額與 GDPR 所追求之同等制裁有異曲同工之妙，當可降低處罰差異化，具裁罰同一性特色。

然而我國受限於現行個人資料保護法的規範，對於違法行為之行政罰鍰其最高額僅為新臺幣 50 萬元，與 GDPR 之高額罰鍰相比，差距相當懸殊，對個案之勸阻力似嫌不足，因此在現有的法規架構下該如何強化對於違法行為的制裁與具勸阻性是一門課題；現階段國家通訊傳播委員會係以前所揭示之「違法行為評量表」及「罰鍰額度參考表」對通訊傳播事業在違法行為之評量，然而將該等評量表及參考表與 GDPR 第 83 條第 2 項 a 至 k 款所揭示之考量標準相較，尚嫌有不足之處，茲說明並整理如下；

A. 違反規則行為之性質、嚴重程度及持續期間，並考量到資料處理之範圍或目的，以及受影響之當事人人數及其受損程度

本款係針對違反規則行為之性質、嚴重程度及該違反行為的持續時間，而參照評量表「考量項目」第一點「對於個人資料之蒐集或處理不具特定目的或不符本法第 19 條第 1 項情形者」及等級劃分[134]，不難看出我國通訊傳播委員會對罰鍰案件進行評量時，亦有參考非目的性處理之情況，及個人資料保護法第 19 條第 1 項各款規定之情形，包含對當事人權益有無侵害的判斷，可知評量表「考量項目」第一點以就違反行為的性質進行考量，並透過等級劃分以判斷該違反行為之嚴重程度，惟就違反行為的持續期間與受侵害的主體人數及受損程度未見有更細節性的評量標準。

B. 違規之故意或過失

本款的內容將違反行為係故意或過失列入裁罰基準，因意圖誤導或販售等行為相較於通常過失行為更為嚴重，反觀評量表中的考量項目均未見對違反行為有故意或過失的區分考量，而係僅針對實施行為其是否違反法律的規定，例如資料之蒐集、處理上是否符合特定目的，或是未取得當事人同意等行為結果，未強調行為當時的主觀要件，此部分可供未來通訊傳播委員會制定評量時列入參考的項目。

[134] 以非常嚴重、很嚴重、嚴重、普通等四個等級作劃分，並透過說明使評量機關得就各等級進行分類，例如達非常嚴重的程度為該違反行為需逾越第 3 次以上命改正期限未改正者。

C. 控管者或受託者為減輕當事人所遭受之損害而採取之任何行動

本款的考量出發點在於當事件發生時，控管者或受託者是否有採取特定的行動以降低災害擴大，而參照評量表「考量項目」第 13 點「違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，未於查明後以適當方式通知當事人」，明列事件發生後未通知為考量標準，然而除了通知外，控管者或受託者仍應採取其他行為，包含聯繫其因錯誤而向第三方共享資料的第三方，以降低個人資料持續外洩的風險，建議未來評量表可將其他補救措施一併列入評量標準。

D. 控管者或受託者之責任程度，需考量到其依據第 25 條和第 32 條所執行之技術性和組織性措施

本款的設計提高了資料控管者在安全維護措施上的責任，包含技術性與組織性措施，而評量表的設計上，不見安全防護措施被納入考量範疇，甚為可惜，預防乃受侵害的第一道防線，建議未來修正評量表可援引我國個人資料保護法施行細則第 12 條之規定，將安全防護措施列入標準，甚至可參考 GDPR 所揭示之原則，制定更全面的安全防護網。

E. 控管者或受託者過去任何相關之違反規則行為

本款的考量基準可對照評量表「考量項目」第（二）點「受

處分人 3 年內受裁處次數：20 分（第（一）項中之第（18）小項除外），此考量項目亦將 3 年內違反行為納入評量標準，有助提高裁罰的嚇阻效果。

F. 與監管機關之配合程度，以改正違反行為並減輕違反行為可能產生之不利影響

本款的內容係將資料控管者與監管機配合程度納入考量，此點可參照評量表「考量項目」第 18 點「通訊傳播事業及其相關人員，規避、妨礙或拒絕本會依本法第 22 條第 1 項、第 2 項之進入、檢查或處分」，該項目亦明定主管機關欲對資料控管者依法行相關檢查時，若資料控管者不願意配合即應列入裁罰，在此部份上評量表項目與 f 款有相似之設計，不同之處在於 f 款仍將改正或減輕違反行為列入審酌，而評量表卻沒有，此點建議未來在修正評量表時可納入參考，以提高資料控管者對於改正違反行為之意願。

G. 受違反規則行為影響之個人資料類型

本款強調當違反行為影響之個人資料類型是特殊類型時，亦將被單獨列為考量裁罰之指標；而評量表中未見對受侵害之個人資料進行分類，未來在修正評量表時建議列入審酌，蓋因特種個資明訂於我國個人資料保護法第 6 條，該等資料受侵害對於當事

人的權益影響重大，單獨列為考量標準加重處罰的效果，將有助於降低特種個資受侵害之風險。

H. 監管機關得知違反規則行為之方式，尤其係控管者或受託者是否就該違反行為進行通知，以及通知之程度為何

本款部份包含事件發生後監管機關得知方式，以及控管者的通知義務，此點在評量表上誠如前面 c 所言，在「考量項目」第 13 點已將通知義務列入評量基準，然而尚未將是否向主管機關通報等主管機關得知違反規則行為方式列入，建議可就評量表內容進行適度修正。

I. 先前已就有關同一主題事件，向相關控管者或受託者發布命令，要求其遵守第 58 條第 2 項所述之措施

本款部份係衡量該違反行為過去就同一主題事件有無被發布其他命令，此點在評量表上可參考說明中臚列之「命改正」，因此評量表中的裁罰仍會就主管機關是否已先為其他措施為參考，此部份與 i 款的內容即為相似。

J. 遵守依據第 40 條認可之行為守則或依據第 42 條認可之認證機制

本款內容主要係將 GDPR 第 40 條的行為守則及第 42 條的認證納入裁罰參考，而通訊傳播委員會的評量參考表則無此部份內容，建議未來修正評量表時可將要求資料控管者是否行認證等

措施列入，得間接強化資料控管者在個資控管上的管理機制。

K. 適用於案件情狀之任何其他加重或減輕因素，例如直接或間接從違反行為中獲得或避免損失之經濟利益

本款屬類似其他標準的彈性事項，此部份可參照評量表「考量項目」第（三）點「其他判斷因素」，兩者均保留裁量上的彈性，賦予主管機關在評估裁罰時一定的自由度，避免裁罰流於僵化。

茲將前述內容，略以下表標示：

GDPR 裁罰考量基準	評量表是否列入
a. 違反之性質、嚴重程度和持續期間	部份相似
b. 違規之故意或過失	X
c. 控管者或受託者為減輕當事人所遭受之損害而採取之任何行動	部份相似
d. 控管者或受託者之責任程度，需考量到其依據第 25 條和第 32 條所執行之技術性和組織性措施	X
e. 控管者或受託者過去任何相關之違反規則行為	V
f. 與監管機關之配合程度，以改正違反行為並減輕違反行為可能產生之不利影響	部份列入

g. 受違反規則行為影響之個人資料類型	X
h. 監管機關得知違反規則行為之方式，尤其係控管者或受託者是否就該違反行為進行通知，以及通知之程度為何	部份列入
i. 先前已就有關同一主題事件，向相關控管者或受託者發布命令，要求其遵守第 58 條第 2 項所述之措施	V
j. 遵守依據第 40 條認可之行為守則或依據第 42 條認可之認證機制	X
k. 適用於案件情狀之任何其他加重或減輕因素，例如直接或間接從違反行為中獲得或避免損失之經濟利益	V

資料來源：本計畫製表

3、 其他矯正措施

與 GDPR 相同，我國個人資料保護法第 48 條亦賦予主管機關對違反行為有限期改正之職權，因此主管機關應優先對違反個人資料保護法之控管者或受託者行限期改正之要求，待其等於期限內未為改正時，即得對其等處以行政罰鍰。此部分之條文內容與 GDPR 在對違反行為施以制裁時，並非全部均立即以行政罰鍰處置之原則相似，

GDPR 亦賦予監管機關一定之告誡、警告、禁令等其他矯正措施，避免逕行處以高額罰鍰而致控管者或受託者造成莫大的衝擊；而較特別的差異在於 GDPR 就違反行為可同時為告誡、警告、禁令等其他矯正措施外，亦可以行政罰鍰行同步處罰，我國在行政裁罰上，因受限於個人資料保護法的規定，僅有限期改善與行政罰鍰的規定，因此無法如同 GDPR 一次為多種矯正手段，建議未來可考慮提升行政裁罰手段的廣度，以強化嚇阻力與適當性。

（五）結論與建議

1、 有效、適當且具勸阻性

如前所言，有效、適當且具勸阻性乃 GDPR 對於違反行為處以矯正措施之主要原則，因此鉅額罰鍰並非其絕對的處罰指標，其他的矯正措施包含告誡、警告、禁令等亦屬得作為勸阻違反行為再次發生之手段，且可視情節輕重同步實施，以確實發揮嚇阻效果。

此外，GDPR 的適用範圍廣泛，除了對設於歐盟各會員國境內之機構之資料控管者或受託者有一體適用外，對於設在歐盟各會員國境外機構之資料控管者或受託者，如在跨境提供商品或服務時，有涉及或處理歐盟各會員國居民的個人資料時，仍應遵守 GDPR 的規範，否則將有鉅額的行政罰鍰，因此，GDPR 的問世與施行，對於全球性的衝擊與影響深遠。

為了有效的嚇阻違反行為的發生，GDPR 除了最高額 2000 萬歐元的高額行政罰鍰外，對於企業亦可課以前一會計年度總營業額 4%之金額，並以最高者計，等於是向全球宣示 GDPR 對個人資料保護的重視，其不僅範圍廣泛，亦非常嚴格。

2、 參考國內其他法規範提高罰鍰額度

就罰鍰金額上，前以提出現行通訊傳播委員會之罰鍰處理要點與 GDPR 進行比較，惟該要點之行政罰鍰係依據個人資料保護法明定之 50 萬元上限，然此罰鍰金額明顯過低，對業者的難以達成有效、適當具勸阻性的效果，因此在修法提高個人資料保護法行政罰鍰前，本研究建議參考近年來金融監督管理委員會對個資裁罰及處分之方式，以保險業為例，2019 年 5 月 17 日南山人壽保險股份有限公司，其因資安管理及投保用戶個資防護上有缺失，當時金管會援引保險法第 171 條之 1 第 4 項以未建立或未執行內部控制或稽核制度對其裁罰 240 萬元整，類似案件有 2015 年 6 月 16 日公勝保險經紀人股份有限公司，其因未訂定個人資料保密處理程序，金管會乃援引保險法第 167 條之 2、167 條之 3 對其罰處 120 萬元整；而「電信管理法」[135]第 9 條就用戶或使用電信人使用電信服務所生通信紀錄及帳務紀錄之保存使用辦法、第 39 條公眾電信網路使用管理辦法、第 50 條專用電信網路使

[135] 民國 108 年 6 月 26 日經總統公布，施行日待行政院制定。

用管理辦法、第 57 條無線電頻率之使用管理規則等授權由主管機關制定相關使用管理辦法，並於同法第 77 條至 79 條規定違法前揭管理辦法可處新臺幣 10 萬元以上 100 萬元以下之行政罰鍰，並得按次處罰之，因此本研究建議未來國家通訊傳播委員會在制定管理辦法時，要求業者建構企業內部對於個資管理的防護機制，並導入 GDPR 技術性及組織性措施的精神，使電信業者對個人資料的保護整體強化，執行裁罰時可參考如同金融監督管理委員會對於保險業、銀行業的裁罰，以電信管理法的罰鍰金額，當可稍微彌補目前個人資料保護法行政罰鍰最高限額威嚇力不足之效果。

3、 修改評量表

最後，參考前揭評量表與 GDPR 裁量基準之比較，建議在相關管理辦法制定及個人資料保護法修法前，國家通訊傳播委員會得透過適度性的修改評量表的裁罰標準，在現有的個人資料保護法框架下，將不足處列入評量，例如增加個人資料保護法施行細則第 12 條所示之安全維護措施，若通訊傳播業者未確實建構此等安全維護措施時，可列入嚴重之違反行為，以加重業者之義務及嚇阻性；另外對於違反行為的故意與過失為區別、列入受侵害個人資料的類型等，納入評量標準，嚴格要求業者對自我行為的控管，使評量表之修改朝有效、適當且具勸阻性的方式前進，逐步合乎 GDPR 行政裁罰之主要原則。

最後，由於 GDPR 仍有相當的新穎性，在實務上的運作，例如同等的制裁該如何操作、一致性的罰鍰適用標準為何等，均有待歐盟第 29 條資料保護工作小組持續訂定規範加以補充，我國應持續且密切的觀察其施行情形與未來走向，現行之相關法規範應持續調整以因應。

肆、物聯網隱私議題

一、機上盒與收視行為

（一）研究動機

於委託機關委託本研究團隊辦理之通傳事業個資管理機制與資料加值處理研討會中，有線電視業者曾詢問收視行為紀錄是否屬於個人資料，並反應有利用雙向機上盒蒐集並處理收視行為紀錄之需求，惟目前我國尚無相關函釋上列疑義，是本研究團隊整理比較相關法制規範如下，供委託機關參考。

（二）概述

有關收視行為之法律規範，可追溯至 1980 年代，當時美國因聯邦最高法院大法官提名人 Robert Bork 法官個人 146 筆影帶租借記錄被記者刊登於《華盛頓城市報（*Washington City Paper*）》而引起軒然大波，為了防止相同事件再度發生，針對個人收視行為所涉及之隱私問題，而制定了「視訊隱私保護法（Video Privacy Protection Act，VPPA）」[136]。另外，針對有線電視收視行為，為了保障消費者之隱私權，美國於 1984 年修正 1934 年通訊傳播法（Communications Act of 1934）並增訂「有線通訊傳播(Cable Communications)」專章，於專章內特別訂定「有線電視隱私法（Cable TV Privacy Act，CTVPA）」，以保護有線

[136] U.S., Video Privacy Protection Act, https://epic.org/privacy/vppa/ (Last visited Nov.18, 2019)

電視消費者之隱私權。而為了因應網際網路科技之蓬勃發展，擬於2020 年 1 月 1 日施行之「加州消費者隱私保護法(California Consumer Privacy Act 2018,CCPA)」則為美國各州首部一般性之個人資料保護法，將增加業者蒐集消費者個人資料之限制，故本研究將節錄部分重要內容，提供委託機關參考。

另於 2017 年有一值得關注之重要案例，即美國聯邦貿易委員會（Federal Trade Commission，FTC）因美國第二大智能電視製造商與銷售商 Vizio 涉及未經當事人同意即蒐集消費者之收視行為紀錄、且將該數據販售予第三人，而向美國紐澤西州地方法院起訴。據 FTC 於同年 2 月 6 日宣布，Vizio 已同意支付 220 萬美元（約新台幣 6,839 萬元）與 FTC 達成和解[137]，這也敲響了隱私安全的警鐘，使業者不得不開始重視消費者之權益。

以下將介紹與分析美國法制重要內容。

（三）美國「視訊隱私保護法（VPPA）」法規內容

1、定義

(1) 消費者（consumer）[138]

由視訊內容服務提供者所提供之產品或服務之租借者、購

[137] 見 https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it (Last visited Dec.20, 2019)

[138] 18 U.S. Code §2710(a)(1):"the term 'consumer' means any renter, purchaser, or subscriber of goods or services from a video tape service provider;"

買者或訂閱者。

(2) 個人可識別資訊（personally identifiable information）[139]

包含識別「向視訊內容服務提供者要求、取得特定視訊資料或服務」之人之個人資料。

(3) 視訊內容服務提供者（video tape service provider）[140]

係指任何參與出租、銷售或傳遞預錄影像卡帶或類似視聽資料之事業，及從事或影響該等跨州、跨國交易之個人；或因視訊內容服務提供者第 b 條第 2 項第 D 款[141]或第 b 條第 2 項第 E 款[142]之行為而接受資料的個人或實體，於該資訊範圍內，亦屬視訊內容服務提供者。」

2、行為規範

(1) 事前告知與書面同意

依據 VPPA 第 b 條第 2 項第 B 款規定[143]，視訊內容服務提供者

[139] 18 U.S. Code §2710(a)(3):" the term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider;"
[140] 18 U.S. Code §2710(a)(4):"the term 'video tape service provider' means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.
[141] 18 U.S. Code §2710(b)(2)(D):"to any person if the disclosure is solely of the names and addresses of consumers and if— (i) the video tape service provider has provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure; and (ii)the disclosure does not identify the title, description, or subject matter of any video tapes or other audio visual material; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;"
[142] 18 U.S. Code §2710(b)(2)(D):"to any person if the disclosure is incident to the ordinary course of business of the video tape service provider;"
[143] 18 U.S. Code §2710(b)(2)(B):" to any person with the informed, written consent (including through an electronic means using the Internet) of the consumer that—(i)is in a form distinct and separate from

除非取得消費者書面同意，否則不得揭露消費者之個人可識別資訊；而取得同意之時點由消費者選擇，可於揭露行為之前，或以特定期間為事前同意，該期間以不超過兩年或是至消費者撤銷其同意時為限，以先到達之時點為準。

另關於同意之撤銷，消費者可選擇針對單一具體個案撤銷其同意，或是對於後續所有揭露行為之同意為一次性之撤銷。

(2) 利用特定資料之要件與例外

依據 VPPA 第 b 條第 2 項第 D 款規定[144]，只要視訊內容服務提供者以清楚、明瞭之方式給予消費者拒絕之機會，得於未涉及任何視訊資料之名稱、描述、主題或其他視訊資料內容之情況下，對他人揭露消費者之姓名及地址；若僅對消費者直接行銷商品或服務，上開有關視訊資料內容之揭露則不在此限。

3、民事責任

依據 VPPA 第 b 條第 1 項第 C 款規定[145]，視訊內容服務提供者故意向他人揭露消費者之個人可識別資訊，當事人可請求其負擔下列

any form setting forth other legal or financial obligations of the consumer; (ii)at the election of the consumer—(I)is given at the time the disclosure is sought; or (II)is given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner; and (iii)the video tape service provider has provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election;"

144 18 U.S. Code §2710(b)(2)(D)

145 18 U.S. Code §2710(b)(1)(c):"to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;"

民事責任：

(1) 實際損害且每件不低於 2500 美元之約定違約金（liquidated damages）；

(2) 懲罰性違約金（punitive damages）；

(3) 合理之律師費用、訴訟費用；與

(4) 賦予法院得裁定適當衡平救濟措施之權利。

（四）美國「有線電視隱私法（CTVPA）」法規內容

1、 定義

(1) 個人可識別資訊 (personally identifiable information)[146]

指**不包含**任何不能識別特定個人之群集資料（aggregate data）。

(2) 其他服務（other service）[147]

指包含有線電視系統業者之任何設備所提供的任何有線及無線通訊服務。

(3) 有線電視系統業者（cable operator）[148]

[146] 47 U.S. Code §551(a)(2)(A):"the term 'personally identifiable information' does not include any record of aggregate data which does not identify particular persons;"
[147] 47 U.S. Code §551(a)(2)(B):"the term "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;"
[148] 47 U.S. Code §551(a)(2)(C):"the term "cable operator" includes, in addition to persons within the definition of cable operator in section 522 of this title, 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."

指包含第 522 節所訂之有線電視系統業者[149]，以及由有線電視系統業者控制、所屬人員，以及任何有線通訊傳播服務提供者。

2、 行為規範

(1) 事前通知與書面同意

依據 CTVPA 第 a 條第 1 項規定[150]，有線電視系統業者與消費者於簽訂收視契約時與契約期限內，每年至少一次，以獨立之書面聲明，清楚、明瞭地告知訂閱者有關已蒐集與將蒐集之個人可識別資訊以及相關利用行為；相關揭露行為、頻率與目的，以及揭露的對象類型；資料保存期限；消費者得近用（access）相關資料的時間與地點；有線電視系統業者關於資料蒐集、揭露所受之限制，以及消費者所享有之權利。

(2) 蒐集個人可識別資訊之要件

依據 CTVPA 第 b 條規定[151]，未取得消費者之事前書面或電子同

[149] 47 U.S. Code §552(5):"the term "cable operator" means any person or group of persons (A) who provides cable service over a cable system and directly or through one or more affiliates owns a significant interest in such cable system, or (B) who otherwise controls or is responsible for, through any arrangement, the management and operation of such a cable system;"

[150] 47 U.S. Code §551(a)(1): At the time of entering into an agreement to provide any cable service or other service to a subscriber and at least once a year thereafter, a cable operator shall provide notice in the form of a separate, written statement to such subscriber which clearly and conspicuously informs the subscriber of—(A)the nature of personally identifiable information collected or to be collected with respect to the subscriber and the nature of the use of such information;(B)the nature, frequency, and purpose of any disclosure which may be made of such information, including an identification of the types of persons to whom the disclosure may be made;(C)the period during which such information will be maintained by the cable operator;(D)the times and place at which the subscriber may have access to such information in accordance with subsection (d); and(E)the limitations provided by this section with respect to the collection and disclosure of information by a cable operator and the right of the subscriber under subsections (f) and (h) to enforce such limitations.In the case of subscribers who have entered into such an agreement before the effective date of this section, such notice shall be provided within 180 days of such date and at least once a year thereafter.

[151] 47 U.S. Code §551(b):" (1)Except as provided in paragraph (2), a cable operator shall not use the

意，有線電視系統業者不得利用有線電視系統蒐集消費者之個人可識別資訊，但為提供服務或調查非法接收訊號者不在此限。

(3) 揭露個人可識別資訊之要件

依據 CTVPA 第 c 條規定[152]，未取得消費者之事前書面或電子同意，有線電視系統業者不得向第三人揭露個人可識別資訊，且應採取適當之安全措施防止非法存取個人可識別資訊之第三人，如其他消費者或其他有線電視系統業者。

有線電視系統業者得於符合下列情形下，揭露個人可識別資訊：

A. 當有線電視系統業者為消費者提供或進行合法商業行為所必要；

B. 於符合同條第 h 項規定[153]之情形下，依據法院命令所授權須揭露

cable system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned.(2)A cable operator may use the cable system to collect such information in order to—(A)obtain information necessary to render a cable service or other service provided by the cable operator to the subscriber; or (B)detect unauthorized reception of cable communications."

[152] 47 U.S. Code §551(c):"(1)Except as provided in paragraph (2), a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator. (2)A cable operator may disclose such information if the disclosure is—(A)necessary to render, or conduct a legitimate business activity related to, a cable service or other service provided by the cable operator to the subscriber;(B)subject to subsection (h), made pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed; (C)a disclosure of the names and addresses of subscribers to any cable service or other service, if—(i)the cable operator has provided the subscriber the opportunity to prohibit or limit such disclosure, and(ii)the disclosure does not reveal, directly or indirectly, the—(I)extent of any viewing or other use by the subscriber of a cable service or other service provided by the cable operator, or(II)the nature of any transaction made by the subscriber over the cable system of the cable operator; or (D)to a government entity as authorized under chapters 119, 121, or 206 of title 18, except that such disclosure shall not include records revealing cable subscriber selection of video programming from a cable operator."

[153] 47 U.S. Code §551(h):"…governmental entity may obtain personally identifiable information concerning a cable subscriber pursuant to a court order only if, in the court proceeding relevant to such court order— (1) such entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and (2) the subject of the information is afforded the opportunity to appear and contest such entity's claim."

之資訊，並應使消費者知悉該命令及收受資訊之第三人；

C. 於有線電視系統業者已提供消費者拒絕或限制之機會，或於有線電視系統業者之直接或間接揭露行為不涉及有線電視與其他服務之視聽與相關資料、任何消費者使用有線電視與其他服務相關交易資訊之情形下，得揭露消費者之姓名與地址。

D. 另有線電視系統業者提供予法定授權之政府機關[154]之資訊，應不包含訂閱者之收視節目紀錄。

(4) 更正、刪除個人可識別資訊之權利

依據 CTVPA 第 d 條規定[155]，有線電視系統業者應提供合理機會予消費者更正其個人資料；於個人可識別資訊蒐集之目的消失時，或因法院須揭露之個人可識別資訊之命令失效時，或消費者要求時，有線電視系統業者應銷毀消費者之個人可識別資訊[156]。

3、 民事責任[157]

因違反 CTVPA 規定，而受損害者，得向有線電視系統業者提起

[154] 18 U.S. Code §119, §121, §206
[155] 47 U.S. Code §551(d):" A cable subscriber shall be provided access to all personally identifiable information regarding that subscriber which is collected and maintained by a cable operator. Such information shall be made available to the subscriber at reasonable times and at a convenient place designated by such cable operator. A cable subscriber shall be provided reasonable opportunity to correct any error in such information."
[156] 47 U.S. Code §551(e):" A cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (d) or pursuant to a court order."
[157] 47 U.S. Code §551(f):"(1)Any person aggrieved by any act of a cable operator in violation of this section may bring a civil action in a United States district court. (2)The court may award—(A)actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;(B)punitive damages; and(C)reasonable attorneys' fees and other litigation costs reasonably incurred…"

民事訴訟請求相關損害賠償，包含但不限於：

(1) 實際損害且不低於約定違約金（liquidated damages），以每日 100 美元或每件 1000 美元計，以最高額為準；

(2) 懲罰性損害賠償金（punitive damages）；

(3) 合理之律師費用、訴訟費用。

（五）美國「加州消費者隱私保護法（CCPA）」法規內容[158]

1、「個人資料」之定義

依據 CCPA 規定[159]，個人資料係指任何識別、關聯、描述，得直接或間接足以連結或可連結至特定消費者或家戶之資料，包含但不限於唯一個人識別碼、網際網路識別 IP 位址、電子信箱、帳戶名稱、社會安全碼、金融資訊（例如購買紀錄）、網際網路或其他電子網路活動資訊等。但不包含已經去識別化或群集消費者資料。

158 本法增訂於加州民法第三篇第四部份第 1.81.5 章。

159 U.S., 1.81.5 Civil Code §1798.140(o)(1):"“Personal information” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following: (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers. (B) Any categories of personal information described in subdivision (e) of Section 1798.80. (C) Characteristics of protected classifications under California or federal law. (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies. (E) Biometric information. (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an Internet Web site, application, or advertisement. (G) Geolocation data. (H) Audio, electronic, visual, thermal, olfactory, or similar information. (I) Professional or employment-related information. (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99). (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.”

2、 告知義務

依據 CCPA 規定[160]，企業於蒐集前或蒐集時，應告知當事人蒐集之個人資料類型及目的；於告知前，不得蒐集或為其他目的之利用。

3、 當事人權利

(1) 近用權

依據 CPPA 規定[161]，企業於接受經核實之消費者要求近用其個人資料時，應立即採取措施向消費者免費揭露與提供本節要求之個人資料，包含近 12 個月內企業基於行銷目的所蒐集該當事人之個人資料類型、資料來源與揭露之第三人類型[162]。

(2) 刪除權

依據 CCPA 規定[163]，消費者得要求企業刪除其消費者蒐集之有關

[160] U.S., 1.81.5 Civil Code §1798.100(b):" A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section."

[161] U.S., 1.81.5 Civil Code §1798.100(d):" A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period."

[162] U.S., 1.81.5 Civil Code §1798.130(a):"(3) For purposes of subdivision (b) of Section 1798.110:(A) To identify the consumer, associate the information provided by the consumer in the verifiable request to any personal information previously collected by the business about the consumer.(B) Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected.

[163] U.S., 1.81.5 Civil Code §1798.105:"(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.(b) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (A) of paragraph (5) of subdivision (a) of Section 1798.130, the consumer's rights to

消費者之任何個人資料，且企業應揭露消費者得要求刪除其個人資料之權利。

(3) 拒絕販售權[164]

消費者有權隨時拒絕企業販售其個人資料，此權利亦可被稱為「選擇退出權」。企業應經當事人事前同意加入，始可將其加入經濟誘因計畫，且當事人可隨時撤銷其同意。[165]

（六）研究發現與結論

1、「收視行為紀錄」是否為個人資料

(1) 否定說：

A. 機上盒通常以「家戶」作為申裝單位，目前業者所蒐集之收視行為紀錄，僅可知悉「家戶」偏好收視之類型、節目，而無法識別實際收視者之身分。

B. 美國第三巡迴上訴法院於判斷個人資料之「間接識別性」，似乎都未特別區分不同的識別主體，而以「大多數人」或「一般人」的角度來觀察識別特定個人的難易程度[166]，亦即對於

request the deletion of the consumer's personal information…"

[164] U.S., 1.81.5 Civil Code §1798.120:" (a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt out."

[165] U.S., 1.81.5 Civil Code §1798.125(b)(3):" A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.135 which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time."

[166] In re Nickelodeon Consumer Privacy Litigation，UNITED STATES COURT OF APPEALS FOR THE THIRD CIRCUIT，https://epic.org/amicus/vppa/nickelodeon/ (Last visited Dec.16, 2019)

大多數人或一般人不具識別性之資料，不應視為「個人可識別資訊」。

(2) 肯定說：

A. 根據美國聯邦貿易委員會與智能電視製造商與銷售商 Vizio 之案例，紐澤西地方法院認為業者蒐集、共享消費者之收視資料應先告知當事人並取得當事人之同意。

B. 歐洲法院曾指出個人資料應包含「已識別」與「可識別」當事人有關之資料，一項資料是否得視為個人資料，不必然以該資料本身可與特定當事人連結，或導致特定當事人被識別為限，應將其他可能合理使用的方法皆納入考量。換言之，雖機上盒蒐集收視行為記錄有可能僅得識別為某一家戶，然仍不能排除有識別特定個人之可能，例如獨居戶，故「收視行為紀錄」既有可能得以訂戶資料、帳單付款資訊等進行比對而識別特定個人，則應類推動態 IP 位址，同屬可間接識別之個人資料。

(3) 結論：以國際法制趨勢而言，多採肯定說。

2、 我國法規調適建議

上述比較法規的重要共同原則共有三點值得我國參考：

(1) 服務提供者於事前告知之義務。

(2) 處理個人資料應取得當事人同意。

(3) 消費者於事後選擇退出之權利。

是以，雖然「收視行為紀錄」是否為個人資料於實務上仍有疑義，然為保護當事人之權益，仍應提醒業者應以嚴謹之態度處理消費者之「收視行為紀錄」，並應課予處理個人資料相同之義務，始符合國際法制趨勢。

復按依據我國電信法第 42 項第 1 項訂定之固定通信多媒體內容傳輸平臺機上盒技術規範 5.13 規定以及有線電視廣播法第 22 條訂定之有線電視終端設備技術規範 5.14 規定：「具收視資料上傳頭端者，收視資料內容不可含有個人資料保護法所指可直接識別個人之資料。」可知目前規範係一律禁止收視資料內容含有可直接識別個人之資料，惟不排除業者未來有可能須以蒐集「個人」之收視行為紀錄之方式提供創新應用服務，例如利用機上盒 TV mail 推播功能與消費者進行互動、與電子商務服務連結等。

是以，建議委託機關仍應考量是否參考 VPPA、CTVPA 等規範之重要共同原則以鬆綁相關法規，允許業者於事前履行告知義務、取得當事人之同意、提供消費者事後選擇退出之方式，以及確保業者已建置「適當安全維護措施」之前提下，始可合理蒐集、處理及利用收視行為紀錄，除了使當事人權益可受到保障之外，亦可促進產業未來發

展之可能，共創「三贏」局面（產業、消費者與主管機關）。

二、智慧家庭物聯網裝置

（一）研究動機

物聯網（Internet of Things, IoT）是當今科技發展的主流，然而在物聯網技術高度發展的環境下，人們每天都可能隨時被許多感知器所圍繞，包括各種智慧家電、消費電子產品及個人使用裝置等，可能在不知情的情況下被這些感知器所偵測，甚至追蹤、監控，尤其當這些物聯裝置透過不同的資料庫連結比對，即可得知使用者個人的偏好、習慣與行為模式時，倘若資料遭到不當的利用，使用者的隱私將會造成威脅[167]。

自 2017 年開始，我國的通訊傳播委員會（National Communications Commission, NCC）為因應 IoT 所涉之資源與監理，除籌劃備妥頻率及號碼等資源外，亦放寬實驗研發測試申請程序及相關電信監理措施、開放低功率廣域物聯網射頻器材型式認證[168]等，藉此促進我國物聯網產業與國際接軌；然而，新興技術的發展亦可能為當今社會帶來包含資安問題、個人資料隱私外洩等風險，NCC 在放寬物聯網射頻器材的同時，是否有因應對策以面對此瞬息萬變的科技

[167] 葉志良，因應物聯網發展資料保護法制的革新—歐盟法制的發展與啟示，中原財經法學第 40 期，2018 年 6 月 11 日，頁 64。

[168] Wi-Fi、Bluetooth、NFC、RFID 等區域型網路技術雖已可因應物聯網萬物相連之需求，但其傳輸距離有限，僅適合室內或特定區域使用。為促進物聯網之發展，NCC 爰據以修正低功率射頻電機技術規範，將原僅適用於區域型之低功率器材，擴增至廣域型之物聯網各種器材亦可適用。詳參國家通訊傳播委員會 2017 年 6 月 7 日新聞稿：https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&cate=0&keyword=&is_history=1&pages=2&sn_f=37492 （最後到訪日 2019.12.15）。

社會將成文本研究的問題核心。

（二）概述

物聯網的概念係 2005 年被正式提出，自美國聯邦交易委員會（Federal Trade Commission, FTC）[169]2015 年發布的報告中，指出物聯網係物體透過設置小型感知器及有線或無線的技術，經由網際網路的串聯並創造無所不在的運算生態系統，而過去對物聯網的研究主要專注在物體間如何運算、偵測、互動並處理數據，對於物聯網技術所帶來的隱私安全風險著墨較少[170]。

近年來，物聯網技術已成為當代發展趨勢，從我國 NCC 開放低功率廣域物聯網射頻器材型式的認證中，我們可以了解物聯網所涵蓋的範圍相當的廣，尤其當感知器結合射頻模組，即可將其所偵測或蒐集之資訊以無線方式傳送至閘道器（Gateway）或基地台，再由後端網路將資料回傳至控制中心或雲端，即時提供業者所需資訊，並推出相關且多元的應用服務[171]，如商業經營可透過無線射頻辨識功能以監控商品庫存、飯店藉由感應系統以監控電力裝置等；特別是在與人工智能（AI, Artificial Intelligence）技術結合後，家庭環境系統的需求對物聯網技術倚賴大增，舉凡智慧音箱、智慧監控系統、智慧電視、智

169 又稱聯邦貿易委員會，本文參考政治大學劉定基副教授的翻譯，以聯邦交易委員會稱之，參劉定基，欺罔與不公平資訊行為之規範–以美國聯邦交易委員會的管制案例為中心，公平交易季刊第 17 卷第 4 期，2009 年 10 月，頁 57。
170 Internet of things Privacy& Security in a Connected World (January 2015), FTC Staff Report at 5.
171 同註 156。

慧冰箱、智慧插座等智慧型家電，均強調藉由物聯網技術，可使生活帶來極高的便利與安全性。

為能更貼近人們生活所需，本研究將著重在智慧家電隱藏的風險以及智慧家電開發者對使用者個人資料之蒐集、存放與加值處理等問題意識，並整理國內外面對物聯網技術對隱私安全造成衝擊的建議，給予主管機關未來建構智慧家電規範時之參考。

（三）應用範圍與問題意識

1、智慧家庭主要內容

(1) 定義

智慧家庭（Smart House，又稱為 Domotics）係物聯網技術的一環，藉由網際網路作為媒介將家庭內部的各物體串聯，形成一個「IoT 自動化平台」，使用者可以輕易地透過科技掌控生活空間，讓家庭環境變得很「智慧」，藉此提高生活品質與舒適度。而網際網路連線為創設智慧家庭環境不可或缺的要素，主要連線設備包含乙太網路、光纖、數據機和 Wi-Fi 路由器，可連接的裝置廣泛，除了最熟悉的智慧門鎖、智慧燈泡、智慧音箱、智慧電視等，就連傳統家電如烤麵包機，也可透過智慧插座增加變化性[172]，這些裝置透過串聯與互動指令，使用數據將

[172] 新型態的生活空間又被稱為複雜 IoT 環境(CIE, Complex IoT Environment)，CIE 內的裝置數

可彙整到「IoT 自動化平台」，進一步達到個人化的智慧家庭環境。

(2) 應用範圍

智慧家庭的應用範圍很廣，從家庭監視系統、智慧門鈴、及各式智慧家電等基本裝置，延伸至生活娛樂、健康照護，均可藉由物聯網的技術而創設智慧家庭環境。目前台灣在應用上，最常見的智慧家庭裝置當屬家庭監視系統，原因在於家庭安全被視為主要需求，家庭監視系統以感知監測居家環境動態，並藉由網路可隨時與手機連動，當居家環境出現異常狀況時，監視系統會立即發出警報，使用者可迅速得知家中異常狀況，除了基本的防盜外，智能家庭監視系統常被應用於寵物動向監控、嬰幼兒夜間監控，甚至災害警報等。

2000 年 6 月韓國的 LG 推出了第一台數位冰箱，這台冰箱以感知器及無線射頻技術，結合商品條碼可以告訴使用者冰箱存放的商品及庫存，此項發明雖是一項創舉，卻因為高成本及不必要性而未造成風潮[173]。2014 年 11 月 Amazon 首次推出 Echo 智慧音箱，開啟人類智能家庭應用的新時代，隨著人工智慧在

量和類型，決定了該環境可提供的指令、互動性及功能，詳細內容可參考資安趨勢部落格：https://blog.trendmicro.com.tw/?p=59959（最後到訪日 2019.12.03）

[173] 周碩彥，「物聯網發展趨勢展示內容」研究報告，國立科學工藝博物館委託研究計畫，頁 2，2015 年 11 月 30 日。

自然語言處理（NLP, Natural Language Processing）技術的突破，透過演算法模型的建立，使電腦能自大數據的建置和訓練過程中歸納出語言的特性，人類不再需要透過打字或觸控等，即可有效的與電腦進行溝通，完成各種應用指令[174]；Amazon 的 Echo 就是透過名為 Alexa 的語音助理，使用者只要輕喚「Hi, Alexa」並以簡單的語音對 Echo 下達指令，Echo 接收指令後就會連結各該指令所涉之相關服務及環境控制，例如撥放音樂、查詢資料、回答天氣等。而隨著科技的演進，智慧音箱的技術也持續精進，全球知名大廠紛紛投入智慧音箱的研發，使智慧音箱的功能從最初期的語音對話，發展至今已可搭載顯示螢幕及適用多人場景等配置，得以連結更多的智能裝置[175]，例如設定電鍋煮飯時間、開關電燈，甚至可以透過智慧音箱進行語音購物。今日，智慧家庭的產品透過 AI 自我學習的技術，已逐漸可以辨識使用者的行為模式而滿足其喜好，如配合使用者的使用習慣執行自動關閉或打開燈光[176]、無線房間感測器可幫助使用者在

[174] 斷開中文的鎖鍊！自然語言處理 (NLP)，中央研究院「研之有物」科普媒體，中研院詞庫小組計畫主持人馬偉雲專訪，詳參 http://research.sinica.edu.tw/nlp-natural-language-processing-chinese-knowledge-information/ （最後到訪日 2019.12.04）

[175] Google 的智慧家庭品牌 Google Nest 即推出一系列的智慧音箱、Apple 的 HomePod 除了撥放音樂、廣播等功能，也可以連結家庭既有的智能配件，幫助使用者輕鬆完成各種需求。

[176] 隸屬於 AMAZON SERVICES LLC ASSOCIATS 計畫的研發團隊推出 BEONHOME 品牌，以居家安全為出發點，開發出智慧門鎖、智慧燈泡等裝置，結合 AI 技術客製化滿足不同使用者的需求，同時扮演守護家庭安全的角色，參考網站：https://beonhome.com/about-us/（最後到訪日 2019.12.04）

不同區域設定不同的溫度，進而達到智慧節能、減少能源耗損的功能。

此外，在高齡化社會下，智慧照顧儼然成為趨勢之一，智慧照顧主要透過網際網路串聯居家感知系統與社區醫療院所，透過醫療院所、長照服務中心與家庭連結，蒐集與分析健康照顧資料，將大量的資料轉化為有用的資訊，幫助長期追蹤監測病患，定期健康管理等，除定時給予使用者照護建議外，當有緊急狀況時亦會發出警示，較常見的如遠距醫療、追蹤失智長者的無線通訊器材、穿戴裝置等[177]均屬之。

2、問題意識

當提及物聯網可能帶來的風險時，主要分為兩個主題，裝置本身的安全防護與個人隱私安全，以下將分別介紹之。

(1) 裝置的安全防護

首先在裝置本身的安全防護上，由於網際網路連線係創設智慧家庭環境的主要媒介，藉由家用路由器形成家庭物聯網，使各項智慧家庭裝置透過家用路由器的串聯形成網絡，然而，家用路由器的防護網不如一般工商業用途來的嚴謹，只要有心人士透過家用路由器，即可任意接觸想要控制的設備，因此若

[177] 吳芳銘，智慧科技列車開進長照，《科學發展期刊》第 554 期，2019 年 2 月，頁 31-32。

爆發網路上的惡意攻擊時，家用路由器將首當其衝成為受攻擊的主要目標。

除了家用路由器以外，在智慧家庭的相關裝置中，用於提升家居生活安全係數的家庭安全設備如智慧門鎖、網路攝影監控等，亦曾被發現該等裝置完全沒有對密碼進行加密或去識別化的相關處理，僅直接以明碼型式儲存密碼，對駭客而言等於沒有任何保護措施，縱使設備本身的性能優異，卻顯現出製造商在設計製造時缺乏資安思維[178]，當使用者個人資料（包含個人生物特徵）透過儲存於各裝置並經由網際網路連線而相互串聯，例如指紋或聲紋被存入各智慧家庭裝置供身分辨識使用，抑或是使用者將網路銀行帳號密碼、信用卡等資訊存入智慧家庭裝置以增加語音購物的便利性等，若裝置或家用網路本身的安全防護不足，駭客的入侵或是裝置受到惡意植入殭屍、木馬等程式，已存入之個人資料外洩的風險便可能存在[179]。

智慧音箱被視為智慧家庭環境的基本配備，使用者可藉由智慧音箱輕易的操控家庭大部分的智慧裝置，包含掃地機器人

[178] 楊玉奇，智慧家庭導入人工智慧強化個資隱私保護之發展現況，行政院「第 5 期發展方案與產業行動計畫(106 年至 109 年)」，https://www.acw.org.tw/Events/Detail.aspx?id=20 （最後到訪日 2019.12.06）

[179] 德國的安全研究實驗室(SRL)在 2019 年 10 月 20 日所發的研究報告即指出 Amazon 的語音助理 Alexa 與 Google Home 的設計因為允許裝設第三方應用程式，當第三方在應用程式通過審查後進行修改並植入惡意程式，使用者的資訊將會因此而受到竊取，詳參 https://srlabs.de/bites/smart-spies/ （最後到訪日 2019.12.06）。

的啟動、空氣清淨機的開關、電視音量的控制等，其背後即代表使用者的使用習慣、行為模式等與智慧裝置產生結合，為生活帶來便利與個人化，然而智慧音箱結合家庭中的各種連網設備，如因裝置本身的設計缺失而引發的資安風險外[180]，使用者個人資料也容易因為物聯網本身的自動化特性，導致使用者對其個人資料的控制程度降低[181]。

(2) 個人隱私安全

在個人隱私安全上，由於 AI 技術的導入，智慧音箱的語音助理極需要大量的數據訓練，以提升語音辨識和應答的準確性，因此智慧音箱開發商在從事商品的研發與改良時，可能正透過現有的設備對使用者的語音內容進行蒐集、研究並分析，此種對於使用者語音內容的使用是否恰當，亦屬值得深思之問題[182]。

再者，不僅是語音內容受到監聽與蒐集，現階段多數的智

[180] 日本電氣通信大學（University of Electro-Communications）和美國密西根大學（University of Michigan）研究員發現，只要駭客用光線接觸到智慧音箱的麥克風設備，就可以透過「光指令」（Light Commands）模式從遠處入侵，甚至可以從另一棟建築物的高處用雷射光穿透窗戶玻璃照射裝置，直接「遠端啟動」設備。詳參：https://www.inside.com.tw/article/18008-iphone-and-homepod-vulnerable-to-line-of-sight-attacks-using-lasers （最後到訪日 2019.12.09）。

[181] 透過物聯網裝置而蒐集到的資料，可能儲存於不同的資料庫內並自動進行比對，將可藉此獲知使用者的特定行為，雖然因為物聯網而使資料的流通與利用的效率提升，卻也易導致使用者對於其個人資料的控制權降低，詳參：Swaroop Poudel, Internet of things: Underlying Technologies, Interoperability, and Threats to Privacy and Security, BERKELEY TECHNOLOGY LAW JOURNAL Vol. 31 at 997.

[182] Bloomberg 報導 Amazon 在訓練 Alexa 時，有大量員工辨識分析數百萬條語音，甚至員工間會共享名人的語音內容，當人類行為的介入，語音助理在提供服務的過程，就會面臨如何保護用戶隱私的問題，詳參：https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio （最後到訪日 2019.12.10）。

慧家庭裝置多需要透過各開發商研發的應用程式（APP, Application）進行操作，除各該應用程式本身的防火牆是否完善外，各開發商可能藉由各裝置或應用程式有定時回傳使用者資料的設計，輕易的獲取個使用者的個人資料（包含生物特徵、醫療照護數據等）或生活習慣，則使用者是否清楚了解開發商的隱私政策、對於個人資料的使用及保存如何蒐集、處理、交換等是否清楚知悉，開發商是否已獲得使用者的同意等都可能存有疑慮[183]；最常見的資料處理在開發商蒐集使用者習慣以用於改善商品本身的缺點並設計出更適合市場之商品，或利用使用者感興趣的領域而對使用者大量投放廣告進行精準行銷，甚至惡意將使用者客人資料對第三方販售，較嚴重的問題是個人資料保存不當而受到駭客入侵[184]等，均涉及到使用者對於其個人資料被處理的範圍是否了解並同意，開發商是否盡到合理使用，且使用者是否已意識到智慧家庭裝置本身存在的資安隱憂等，均為智慧家庭技術在發展過程中所需面對的問題。

（四）各國管制與建議

[183] 2012 年初發生在 iOS 的事件，有應用程式在未經使用者允許或甚至未告知下就從通訊錄裡收集資料，此事件的發生導出 Apple 過去未強制應用程式開發商在存取 iOS 通訊錄時要對使用者提出警告並取得使用者授權，詳參：https://blog.trendmicro.com/oblivious-data-loss-and-the-wild-west-of-mobile-app-security/ （最後到訪日 2019.12.10）。

[184] 2017 年 Uber 使用者資料共 5700 萬筆因駭客入侵而遭竊取，Uber 後來支付 10 萬美金給駭客以換取將使用者資料刪除，詳參：https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data （最後到訪日 2019.12.06）。

由於物聯網技術應用於智慧家庭系統上已為個人隱私的安全防護帶來衝擊，各國的政策制定者或相關的研究員也開始思考如何提升相應的管制或保護措施予以回應，其中，隱私政策開放且透明、數據最小化，以及提供使用者選擇與控制權等基本原則被視為防護關鍵[185]。以下將援引日本、美國、歐盟等國家在面對物聯網技術快速發展時，對於個人隱私安全受侵害而因應之方式，以及美國 FTC 與美國互聯網協會（Internet Society）等機構對監管機關提出之建議等作為本研究之參考。

1、 各國的因應方式

圖 3　各國針對隱私安全保護之因應方式整理表

國　家	因應方式
日　本	1. 制定個人資料保護法（APPI） 2. 設立個人資料保護委員會（PPC） 3. 通過歐盟適足性認證
美　國	1. 依據聯邦交易委員會法第 5 條規定擴張對隱私保護的管制範圍 2. 依據欺罔與不公平資訊行為之規範原則，強化個人隱私保護執行

[185] FTC Staff Report(January 2015), supra note 4, at 5.

	3. 提出「消費者隱私權保護框架」 4. 相應保護措施及裁罰
歐　盟	1. 以 2002/58/EC 號電子通訊隱私指令補充第 95/46/EC 號資料保護指令 2. 依據 GDPR 要求資料控制者採取適當的安全維護措施等
巴西、印度	提出個人資料保護規則草案

(1) 日本

近 15 年來，物聯網技術已經為日本的 GDP 帶來了高達 9 千 6 百億美金的成長，日本亦在國際間被視為全球物聯網生態產業的驅動者，特別是在機器人工業上，2003 年為健全個人資料保護，日本制定一部完整的個人資料保護法（APPI），爾後該法經過部分修正逐步強化個人資料有更明確、廣泛的保護，如設立個人資料保護委員會（PPC），賦予該委員會創建並執行相關隱私規範的權力，以及限制未獲得主體同意的資料不得傳輸至第三方等內容[186]，2018 年 7 月 1 日日本正式通過歐盟 GDPR 的適足性認證，在個人資料保護上與歐盟達成平等雙向

[186] Assessing Regulatory Requirements of Privacy Management for Members Offering IoT Services Using Personal Data(November 2018), GSMA at 18. Available at: https://www.gsma.com/iot/wp-content/uploads/2018/11/GSMA_Assessing-regulatory-requirements-of-privacy-management-for-members-offering-IoT-services-using-personal-data.pdf （最後到訪日 2019.12.10）。

的機制，提高隱私處理標準，亦使日本與歐盟間可自由的傳遞個人資料[187]。

(2) 美國

美國 FTC 一向將消費者的隱私視為消費者保護工作的主要任務之一，自 1990 年末開始，FTC 即鼓勵線上交易業者揭露其資訊行為，並建議業者主動遵守 4 項公平資訊行為原則，這 4 項原則為告知、選擇、查閱、安全，亦即業者應使消費者知悉其個人資料的蒐集使用，並提供消費者選擇是否提供資料做不同於蒐集目的之使用，業者更應賦予消費者查閱、更正資料庫檔案，採取合理措施以保障蒐集資料的安全等[188]；而 2005 年起，FTC 多次利用聯邦交易委員會法第 5 條禁止不公平（unfair）行為的規定，進一步擴張其對隱私保護的管制範圍，舉凡「業者未充分告知其資料蒐集、處理的原則」、或「業者未採行合理適當的資訊安全措施」，均被認定為不公平行為[189]，爾後，FTC 透過聯邦交易委員會法中「欺罔與不公平資訊行為之規範」（Unfair or deceptive acts or practices）原則，用以強化物聯網技術發展後的個人隱私保護執行，確保各物聯網開發商

[187] The GSMA welcomes agreement by the EU and Japan on cross-border data flows(July 2018), GSMA. Available at: https://www.gsma.com/publicpolicy/the-gsma-welcomes-agreement-by-the-eu-and-japan-on-cross-border-data-flows （最後到訪日 2019.12.12）。
[188] 同註 186，頁 60。
[189] 同註 186，頁 58。

在隱私保護聲明應遵循該原則[190]，2012 年 FTC 更提出「消費者隱私權保護框架」，以適用所有商業實體為原則，並提出從「設計著手保護隱私」（Privacy by Design）的概念，鼓勵企業改善內部流程，以利在產品或服務設計之初即納入隱私保護機制[191]。另外，美國除有聯邦政府的相關法規範得遵循外[192]，各州亦有相應的保護措施及裁罰，如 2017 年美國紐澤西州亦曾對電視廠牌 VIZIO 開罰 2 千 2 百萬美金，因 VIZIO 在未告知亦未取得使用者同意下，即任意的蒐集使用者的收視行為數據[193]。因此美國在個人隱私保護上，自 1990 年代開始，即豎立了隱私保護的基本原則，並持續順應時代的發展而修正。

(3) 歐盟

事實上，歐盟過去在第 95/46/EC 號資料保護指令時期，對於個人資料的保護就已相當的重視，而對電子通訊服務下的資料保護與隱私權，則以 2002/58/EC 號電子通訊隱私指令為

190 U.S., FTC Staff Report(January 2015), *supra note 4,* at 14.
191 Protecting Consumer Privacy in an Era of Rapid Change Recommendations for Business and Policymakers (March 2012), FTC Staff Report at 23. 「設計著手保護隱私」此翻譯係參考郭戎晉，隱私法制新趨勢－從設計著手保護隱私（Privacy by Design），科技法律透析第 25 卷第 8 期，2013 年 8 月 15 日，頁 38 以下。
192 如電信通訊客戶隱私可攜行為，美國聯邦通訊委員會透過確立相關的準則以保障之，詳參 Legal Information Institute(2017) Customer Proprietary Network information regulation: https://www.law.cornell.edu/cfr/text/47/part-64/subpart-U （最後到訪日 2019.12.11）。
193 VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent. Available at: https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it （最後到訪日 2019.12.11）。

第 95/46/EC 號指令的補充，爾後，網際網路的高度發展使人與人之間的關係透過資訊流通而緊密相連，資訊隱私特定的使用目的與共享方式受到重視，人們得以在各階段控制個人資料的權利因應而生[194]。2014 年 9 月由 WP29 針對物聯網發展現況提出一份工作小組報告（WP233, Opinion 8/2014 on the Recent Developments on the Internet of Things），此份報告整理了在物聯網應用下隱私安全所面臨的難題，包含使用者難以控制其個資以及所獲得資訊之不對稱、同意權行使困難、對於資料推論與二次利用行為脫逸於原始蒐集目的之外、侵入性辨識使用者行為以及對使用者進行特徵分析、在利用服務時對於維持匿名性造成威脅，以及物聯網安全危機等議題[195]。

2018 年 5 月 25 日在 GDPR 施行後，為全球隱私保護確立了新的標準；GDPR 除要求資料控制者應依據隱私風險程度而採取適當的安全維護措施[196]、資料外洩時必須通知資料當事人等與資料控制者內部流程有關之規範外，亦特別強調資料控管者應取得當事人明確且有效的同意，亦即該同意係賦予當事人對與其有關之個人資料可否被處理之控制權的工具，若個人資

[194] 此權利被稱為資訊自決權，由於網際網路的發展使資料的流通變得迅速，單純賦予人們對於個人隱私使用的同意與否已無法滿足現今資訊社會的趨勢，應盡量使人們在資訊流通的各階段皆可控制其個資被傳遞的範圍與使用，同註 169，頁 82。
[195] 同前註，頁 76-77。
[196] EU, 2016/679/EC, §35(1),.

料被處理係依據當事人無效的同意，則該處理即屬違法[197]；此外 GDPR 要求資料控管者應主動揭露有關處理個人資料的所有資訊（例如隱私聲明或通知），當有增補或變更時亦應主動通知當事人注意增補或變更的內容，此即為個人資料處理的透明性[198]，使資料當事人得知悉控管者處理資料的方式。

(4) 其他國家

除了前面提及的指標國家及區域外，巴西、印度等開發中國家也正在思考建立新的個人資料保護規則，如印度國會在 2018 年釋出一份立法草案，被視為是受歐盟 GDPR 的影響，該草案即試圖在現有的個人資料保護法中對處理個人數據的所有主體賦予新的義務，並且定義「關鍵個人數據」（Critical Personal Data），限制此種關鍵個人數據僅能在印度境內處理，不得對境外傳遞或轉移[199]。

2、監管建議

(1) 資安風險的修復

IoT 智慧家庭裝置的資安風險，最大的問題在於網際網路作為資料傳輸媒介，過去駭客發動 DDoS 攻擊事件，藉由感染監視攝影機、路由器等設備，讓這些裝置作為攻擊來源，進而

197 EU, WP29, Guidelines on consent under Regulation 2016/679 at 3.
198 EU, WP29, Guidelines on transparency under Regulation 2016/679 at 6.
199 GSMA , *supra note 21,* at 20.

直接影響目標系統的運作，使受攻擊的範圍不再只是單一裝置，而是延伸到整體的網絡，因此美國 FTC 在 2017 年上半年度發起了物聯網家庭資安檢查挑戰獎金賽，希望有參與者能設計出一套可替老舊的物聯網裝置，進行檢查、安裝更新與強化密碼防護的系統工具，協助使用者對自己的物聯裝置進行有效的檢查並更新[200]。

此外，美國 FTC 也對裝置的開發商提出相關建議，包含在開發製造初期就應該把安全防護系統放入設計、對員工有完善的資安教育訓練、與使用者間的契約應明訂隱私權條款及資料存放方式、提供更深層且多樣化的防護、置入合理的可控系統等[201]，藉此從開發源頭就為物聯裝置的安全防護把關，避免使用者因自我缺乏防護意識而陷入風險。

(2) 同意權與透明性

有鑑於 IoT 智慧家庭裝置可能延伸各種隱私安全風險，美國互聯網協會在 2019 年 9 月發表了一份政策簡報，簡報中特別就現今的物聯網技術與政策進行說明，並進一步對家庭中持續增加的「互聯裝置」，提出警告，認為物聯網技術的發展將

[200] 最終該競賽由 Steve Castle 團隊設計的 IoT Watchdog 獲得首獎，IoT Watchdog 是一款手機用的 app，使用者可以透過這款 app 對家中的 Wi-Fi 及藍芽進行偵測，確認相連接的裝置為何，並且提供相應的更新軟體以解決相連裝置可能存在的弱點，詳參：https://www.ftc.gov/iot-home-inspector-challenge （最後到訪日 2019.12.10）。

[201] U.S., FTC Staff Report(January 2015), *supra note 4*, at 28.

導致使用者逐漸習慣感應設備的存在，卻遺忘該等裝置可能對隱私的蒐集與侵犯，甚至暴露給第三方即物聯網裝置的開發商而不自知[202]。

互聯網協會就隱私安全的監管建議分為三大類，茲說明如下：

A. 提高使用者控制（Enhance User Control）

首先是提高使用者對於裝置開發商使用個人隱私的控制權（Enhance User Control），由於現階段的智能家庭裝置多配置第三方存放數據，因此提高使用者對於自身隱私數據受使用的控制權力，將有助於減緩其個人隱私在未知下暴露，例如開發商應賦予使用者對於其個人資料被存取有知情同意權，使用者可以自由選擇共享數據的範圍或停止共享數據，且開發商與第三方均須受到同等的隱私政策聲明規範，藉由被賦予相當的控制權，使用者將可有效掌控開發商與第三方存取個人數據的界限，限制隱私數據被使用的範圍。

B. 增進透明度與通知（Improve Transparency and Notification）

[202] 美國互聯網協會指出物聯網技術的發展，使相應的法律還未能跟得上科技進行修法，例如使用者使用穿戴式設備紀錄健康訊息，但是該穿戴式設備卻不受醫療數據法的規範；此外，賦予使用者知悉其隱私被使用的透明度及對隱私的控制權都是必須的，詳參 2019 年 9 月 19 日發表的 Policy Brief: IoT Privacy for Policymakers，https://www.internetsociety.org/policybriefs/iot-privacy-for-policymakers/ （最後到訪日 2019.12.07）。

其次是增進透明度與通知（Improve Transparency and Notification），由於智能家庭裝置的設計多為生活使用上熟悉的物品，例如冰箱、電視、門鈴、音響等，當這些裝置已與生活習慣密不可分時，使用者對於該等裝置在使用同時有紀錄並傳送資料的設計將缺乏警覺，美國互聯網協會即認為現行的物聯網裝置沒有很好的通知方式來告知使用者他們的個人資料正在被蒐集或紀錄，且開發商的隱私政策聲明也不夠透明，因此建議監管單位應要求裝置開發商隱私政策聲明的明確性，讓使用者可了解其隱私資料被使用之目的，被儲存期間及被傳送的地點，另外亦賦予使用者個人資料蒐集同意權及拒絕權，使用者可以隨時選擇其資料被刪除而不被使用。

C. 與時俱進（Keep Pace with Technology）

是隨時與科技保持同步（Keep Pace with Technology）是最重要的，此建議的主要準則是要求相關的法規、政策應該隨時與科技保持同步，如此才能有效的規範智能家庭裝置，避免因為科技的發展，使法規範跟不上科技的腳步，而產生規範上的漏洞，當然如果有一部對整體數據蒐集及使用進行規範的法律是最好的，如此將可以使所有的數據

資料從個別技術中獨立出來，更可透過該法律保障從事隱私研究工作的人不會因為隱私研究而觸犯法律風險[203]。

此外，同意權與透明性的要求亦可從歐盟 GDPR 的規範內窺知，依 GDPR 第 5 條規定，透明性的要求是基本原則之一，主要內容為要求關於個人資料處理之任何資訊或溝通方式應以便於取得、易於理解且使用清晰簡明之語言，尤其控管者應向當事人提供身份、處理資料之目的以及進一步資訊，用以確保資料處理之公正性和透明性，並使個人資料受用得當事人得有權利對個人資料進行確認和溝通[204]，亦即資料控管者的隱私聲明，應該使當事人了解個人資料被處理之內容、處理目的及可能存在的風險，且這些隱私聲明應得使當事人輕易地取得並了解，再者，若資料控管者係從第三方、公眾來源或其他當事人處取得當事人之個人資料，仍須在取得資料後得合理期限內對該當事人提供如前述之隱私聲明相關資訊，以合乎 GDPR 所揭示的透明性[205]。是以，GDPR 在防範維護個人隱私上，特別要求資料控管者的隱私聲明必須明確且透明，甚至取得資料來源非當事人本身，仍應有主動通知當事人的義務，當事人得輕易掌控並了解其個人隱私的處理及可能延伸的風險。

---

203 *Id*.
204 EU, WP29, Guidelines on transparency under Regulation 2016/679 at 6.
205 *Id*. At 14.

在同意權的部分，GDPR 的同意基本觀念與 95/46/EC 指令中的基本觀念相似，依 GDPR 第 6 條規定，同意是資料控管者合法處理個人資料所需依據的根據之一[206]，而在同意權的行使上，GDPR 指出當事人同意必須是出於自由意志，而非建立在權力不對等、或有條件性的，因此確保同意處理個資不可成為契約直接或間接之履行對價亦屬有效同意的內涵[207]。此外有效同意也伴隨著撤回同意權，GDPR 第 7 條第 3 項即規定資料控管者應確保當事人得以與同意相同簡易的方式，在任何特定時間撤回其同意，若此撤回同意權不符合 GDPR 的要求，即代表控管者給予當事人資料處理同意權並不符合 GDPR 的規範，而資料控管者基於透明性義務也應將撤回與同意方式及權利告知當事人[208]。

不論是美國互聯網協會的監管建議抑或是歐盟 GDPR 指令，均可得出為了確實避免 IoT 智慧家庭裝置使用者在使用相關裝置時，使用者對其個人資料可能被開發商或第三方任意的存取處理或卻不自知，甚至個人資料透過網際網路的傳遞，任意的被公開或揭露，因此規範開發商或第三方必須確立明確的隱私政策或隱私聲明，並確實賦予使用者對其個人

206 EU, WP29, Guidelines on consent under Regulation 2016/679 at 4.
207 *Id.* At 6-7.
208 EU, WP29, *supra note 38*, at 21-22.

資料處理之同意或撤回同意等權力是極為必要的，而我國在面對科技發展的洪流下，國家通訊傳播委員會作為物聯網服務的監管機關，該如何在現有法規的架構下，注入隱私安全的防護網將是未來應關注的焦點。

（五）結論與建議

面對物聯網產業的高度發展，我國政府亦將物聯網視為未來經濟市場的主要趨勢，則物聯網為人們所帶來的隱私安全問題即備受重視。事實上，人們對於公共場合與私人空間所享有的隱私期待標準不同，原本私人空間的高度隱私期待卻因為 IoT 智慧家庭環境的設置下，導致個人的居家生活習慣透過物聯網傳遞到全球各地，如此高度入侵私人領域亦使人們對於物聯網裝置產生懷疑，絕大多數的人們並不相信物聯網帶來的好處比其隱私更為重要[209]，因此為促進物聯網市場的發展同時，我國亦應對使用者隱私安全進行相應的保護。

1、推行資安認驗證標章

在我國，物聯網技術仍處於新興發展的階段，面對物聯網設備潛藏的資安風險，我國政府由行政院科技會報即行政院資通安全處指導，積極推動物聯網設備的資安認驗證標章，其中具有線介面之物聯網終端產品資安檢測，由經濟部負責推動；具無線介面或電信、傳播終端

[209] 同註 184，頁 69-71。

設備介面者則由國家通訊傳播委員會主責，藉由三方相互合作制訂物聯網設備資安測試標準、檢測環境及輔導廠商產品進行資安檢測等業務，強化物聯網的安全[210]。

然而，資安危機或許有機會透過物聯網資安認驗證標章解決設備本身安全防護系統的不足，但在個人資料隱私保護上，使用者如何避免時時刻刻受到物聯網裝置對隱私的蒐集與監控成為主要課題。

2、同意權與透明性

本研究認為，我國物聯網裝置的主管機關[211]除了參考美國互聯網協會提出的監管建議，自裝置的開發設計階段即要求開發商應確保裝置本身的安全防護機制外，實際上最重要的為賦予開發商或資料控管者一定的義務，包含公開完備的隱私政策或聲明，給予使用者輕易充分知悉的管道，使用者即可藉此掌握個人資料的流向與被處理的方式，另外亦應要求開發商或資料管控者應獲得使用者明確及有效的同意，且此種同意並非只是過去單純傳統規範之資料被使用的同意，此種同意權是建構在當事人已充分知悉其個人資料被處理的方式與傳遞的

[210] 有關物聯網資安認驗證標章之介紹，詳參台灣資通產業標準協會網頁：http://www.ifantech.net/taics/Validation01.aspx?validateType_id=1#Validation （最後到訪日 2019 年 12 月 19 日）；令經濟部工業局已發展 IPCAM 資安產業標準及檢測規範正式版，此規範可協助業者確保產品符合 IPCAM 產品品質規範，也讓設備製造商與系統服務商在產品研發和設備採用方面均有所依據，自開發源頭即注入資安意識，詳參 http://www.ifantech.net/taics/AnnouncementArticle.aspx?AnnouncementID=1 最後到訪日 2019 年 12 月 19 日）。

[211] 我國現行物聯網目的事業主管機關為經濟部，然而物聯網的應用範圍廣泛，未來政府對於整體物聯網技術的推行是否有其他主管機關的設置，仍值得關注。

範圍，賦予當事人在同意權行使上的彈性[212]。

再者，根據前述之歐盟 WP29 工作小組 2014 年報告指出使用者的「同意權行使困難」是物聯網產業發展的難題之一，WP29 工作小組告報認為在許多情況下使用者根本不知道其資料正在被特定監控物件所蒐集、處理，例如目前許多穿戴式裝置、家庭監控設備等，經常會在使用者不知情的情況下蒐集並傳遞資料，導致使用者對於此種資料處理（蒐集並傳遞資料）難以進行同意[213]；而觀諸我國法規範，我國個資保護法在 2015 年修正後，對於告知同意主要規定在第 7 條、第 8 條、第 9 條、第 15 條、第 16 條、第 19 條以及第 20 條，其中第 7 條第 3 款規定「公務機關或非公務機關明確告知當事人第八條第一項各款應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已依第十五條第二款、第十九條第一項第五款之規定表示同意。」上開規定處理在物聯網環境下，雖服務提供者或裝置物件本身確實已主動告知個資蒐集相關事項，若當事人因為未充分知悉而未表示拒絕，則因推定同意的法律效果，致物聯網裝置自動化處理使當事人的資料已被傳遞、處理[214]，將使當事人難以掌控個人資料的流向

[212] 以具備智慧家庭裝置的民宿業者為例，入住該民宿的人將可能使用該民宿的所有智慧家庭裝置，但是使用者不見得願意將自己使用智慧家庭裝置所建入的個人資料或使用習慣流至第三方，則應該賦予使用者同意權行使的範圍，該範圍不限於全部同意利用，亦可能包含部分同意利用，相似內容可參考註 1，頁 107-108。
[213] 同前註，頁 78。
[214] 同前註，頁 111-112。

與處理，此將成為我國急需解決與深思之課題。

此外，由於 IoT 智慧家庭系統包含家庭照顧，使用者可藉由相關的穿戴式裝置而傳送與身體機能相關的數據，並結合社區醫療或其他智慧裝置以達成家庭照顧的需求，特別在高齡化社會下，此種家庭照顧系統已開始受到注目，然而在我國現行的個人資料保護法下，病歷、醫療、基因、健康檢查等被歸為特種資料，在特種資料的利用上，除符合法規範外，需取得當事人的書面同意，此書面同意雖依個人資料保護法施行細則之規定，可以電子簽章代替，但仍可能使家庭照顧系統在設置上受到某種程度的限制，要如何在特種資料與智慧家庭照顧系統間取得平衡，亦屬未來我國應面臨之課題。

最後，當面對物聯網技術的高速發展，現階段由於我國物聯網產業現階段在推行包含對當事人同意權與透明性等個人隱私安全防護機制上，尚未有明朗的制度，則為確實維護個人資料隱私安全，本研究建議我國應先決定整體物聯網技術與裝置之主管機關，使物聯網技術與裝置得被全面且有效的控管，而在修法前，現行物聯網產業的主管機關即經濟部得透過行政指導的方式，在我國個人資料保護法框架下，協助相關業者制定隱私政策以強化當事人同意權及公開完備的隱私聲明，以提升對隱私安全的保護。

伍、特別法規比較

一、歐盟 e-Privay Regulation 草案

（一）背景

在數位經濟時代下，大數據處理與資訊共享已成為不可逆的趨勢，而全球化的資料流通，勢必也讓個人資料保護面臨更嚴峻的考驗。歐盟於2018年5月全面施行GDPR，建立了一套嚴格的個人資料保護法制架構，亦促使許多國家重新檢討個人資料保護法規[215]。同時隨著網際網路技術處理方式日漸多元，網路服務之商業模式產生巨大變革，許多新型態的網路服務已逐步侵入過往受政府高度監管之產業，例如電信、電視、電台等特許產業，歐盟多數會員國認識到有必要將通訊隱私保護單獨立法規範。有鑑於此，歐盟執行委員會於2017年1月10日提出「歐盟隱私與電子通訊條例草案」（Proposal for a Regulation on Privacy and Electronic Communications，以下簡稱ePrivacy草案），並於持續接受各會員國提出修正建議，以便規範新型態的網路服務業者，此外該草案也對境外電子商務業者提出相對應的規範，具體實踐個人隱私權和個人資料的保護。

ePrivacy草案規範範圍涉及通訊隱私保護，與國家通訊傳播委員

[215] 國家發展委員會，個人資料保護專案辦公室，https://www.ndc.gov.tw/Content_List.aspx?n=726A44EA5D724473（最後瀏覽日：2019 年 12 月 1 日）

會業務職掌密切相關，本團隊認為其內容應有供國家通訊傳播委員會借鏡之價值，因此本團隊額外針對ePrivacy草案進行研究並提出建議。

（二）歐盟隱私與電子通訊條例草案介紹

歐盟委員會最新提出之的ePrivacy草案共七章、二十七條。處理了歐盟第2002/58/EC號指令、歐盟第2009/136/EC號指令規範不明確的問題，及GDPR未能涵蓋的個人通訊隱私保護問題。第一章是總則，主要包括適用範圍和對相關概念的定義；第二章主要針對如何保證電子通訊秘密性以及處理電子通訊資料的條件與目的；第三章賦予使用者控制電子通訊資訊發送和接收的權利；第四章規定該法案的主管機關與部門；第五章則是相關救濟措施以及法律效果；第六章規定相應的委託行為和實施行為；第七章為最終條款，包括廢除電子隱私指令以及新法如何通過與何時生效等問題。內容主要有以下幾點：

1. 擴大監管範圍

依據ePrivacy草案第4條定義規定[216]，歐盟電子通訊準則指令第2條

[216] U.S., ePrivacy 草案, §4 <Definitions>.
1. For the purposes of this Regulation, following definitions shall apply:
(a) the definitions in Regulation (EU) 2016/679;
(b) the definitions of 'electronic communications network', 'electronic communications service', 'interpersonal communications service', 'number-based interpersonal communications service', 'number-independent interpersonal communications service', 'end-user' and 'call' in points (1), (4), (5), (6), (7), (14) and (21) respectively of Article 2 of [Directive establishing the European Electronic Communications Code];
(c) the definition of 'terminal equipment' in point (1) of Article 1 of Commission Directive 2008/63/EC.
2. For the purposes of point (b) of paragraph 1, the definition of 'interpersonal communications service' shall include services which enable interpersonal and

第各點所述包括：電子通訊網路、電子通訊服務、人際通訊服務、以電話號碼為基礎之人際通訊服務、非以電話號碼為基礎之人際通訊服務、終端用戶、呼叫等通訊方式均受該草案管制，其中所謂「非以電話號碼為基礎之人際通訊服務」，將各種即時通訊軟體例如WhatsApp、Facebook Messenger以及Skype等納入到了政府監管範圍，使得新興的通訊技術必須與傳統通訊服務受到同樣強度的監管。

此外，在地域管轄部分，依據ePrivacy草案第4條規定，該本條例適用於向歐盟終端用戶提供付費或免費之電子通訊服務或相類

interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.

3. In addition, for the purposes of this Regulation the following definitions shall apply:
(a) 'electronic communications data' means electronic communications content and electronic communications metadata;
(b) 'electronic communications content' means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound;
(c) 'electronic communications metadata' means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication;
(d) 'publicly available directory' means a directory of end-users of electronic communications services, whether in printed or electronic form, which is published or made available to the public or to a section of the public, including by means of a directory enquiry service;
(e) 'electronic mail' means any electronic message containing information such as text, voice, video, sound or image sent over an electronic communications network which can be stored in the network or in related computing facilities, or in the terminal equipment of its recipient;
(f) 'direct marketing communications' means any form of advertising, whether written or oral, sent to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, etc.;
(g) 'direct marketing voice-to-voice calls' means live calls, which do not entail the use of automated calling systems and communication systems;
(h) 'automated calling and communication systems' means systems capable of automatically initiating calls to one or more recipients in accordance with instructions set for that system, and transmitting sounds which are not live speech, including calls made using automated calling and communication systems which connect the called person to an individual.

似之服務，若電子通訊服務之提供者若非設立於歐盟境內，其應以指派一名歐盟境內之代表人，負責回答相關問題及提供必要資訊，特別是向監管機關、終端用戶提供與處理電子通訊資料相關訊息，且該電子通訊服務提供者，不因本條指定之代表，而免於該服務所衍生之法律訴訟。

2. 秘密通訊保障

依據ePrivacy草案第5條規定[217]，所有電子通訊資料原則應受保密，禁止對用戶電子通訊資料有任何干擾，例如: 聽取、竊聽、儲存、監視、掃描(審視)或其他種類之截取、監管或處理電子通訊資料，同時依據ePrivacy草案第7條[218]，電子通訊服務之提供者在用戶接收電子通訊內容及於通訊傳輸目的消失後，應將該資訊刪除或標

[217] U.S., ePrivacy 草案, §5 <Confidentiality of electronic communications data>
Electronic communications data shall be confidential. Any interference with electronic communications data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.

[218] U.S., ePrivacy 草案, §7 <Storage and erasure of electronic communications data>
1. Without prejudice to point (b) of Article 6(1) and points (a) and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or st，ored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679.
2. Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication.
3. Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2), the relevant metadata may be kept until the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law.

示為匿名，上開資訊可在用戶同意下，由其授權之第三方記錄儲存或以其他方式處理。

依據ePrivacy草案第6條規定[219]，電子通訊服務提供者例外可為執行電子通訊資訊傳遞、維持電子通訊服務安全性以及探測技術故障與錯誤之目的，於必要之期間內處理電子通訊資訊。

3. 限制加密

[219] U.S., ePrivacy 草案, §<Permitted processing of electronic communications data>
1. Providers of electronic communications networks and services may process electronic communications data if:
(a) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or
(b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.
2. Providers of electronic communications services may process electronic communications metadata if:
(a) it is necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/212011 for the duration necessary for that purpose; or
(b) it is necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or
(c) the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous.
3. Providers of the electronic communications services may process electronic communications content only:
(a) for the sole purpose of the provision of a specific service to an end-user, if the end- user or end-users concerned have given their consent to the processing of his or her electronic communications content and the provision of that service cannot be fulfilled without the processing of such content; or
(b) if all end-users concerned have given their consent to the processing of their electronic communications content for one or more specified purposes that cannot be fulfilled by processing information that is made anonymous, and the provider has consulted the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.

[219] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (OJ L 310, 26.11.2015, p.1–18)

為確保政府機構與執法單位可於法定情況下，取得電子通訊資料，ePrivacy草案第11條[220]規定，政府可以基於國家安全、司法調查或其他公共利益等目的，立法限制人民秘密通訊之自由。電子通訊服務提供者應建立適當內部程式，因應政府機構獲取電子通訊資訊之請求，同時此內部程式需建立相應監督機制。

4. 保障使用者行為習慣與設備秘密性

依據ePrivacy草案第8條規定[221]，在沒有使用者同意或其他正當

[220] U.S., ePrivacy 草案, §11 <Restrictions>
1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.
Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. They shall provide the competent supervisory authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.

[221] U.S., ePrivacy 草案, §8 <Protection of information stored in and related to end-users' terminal equipment>
1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:
(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or
(b) the end-user has given his or her consent; or
(c) it is necessary for providing an information society service requested by the end- user; or
(d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end- user.
2. The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:
(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or
(b) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.
The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.
3. The information to be provided pursuant to point (b) of paragraph 2 may be provided in

理由下，禁止利用使用者終端設備之處理與儲存功能（包括硬體和軟體），此部分最常討論之適用情境即係Cookie技術之應用，依據ePrivacy草案第8條第2項第(b)款及第10條之規定，處理Cookie技術時，應該告知終端用戶那些內容，並要求電子通訊服務提供者必須設計不於使用者終端設備儲存Cookie，仍能提供服務之可能及明確的隱私權選項，使終端用戶係於明確知悉自己的同意將會使自己終端設備內被儲存哪些Cookie？及這些Cookie與何種類型之個人隱私權可能相關，且亦能選擇不餘終端設備內儲存Cookie而使用服務，此時終端用戶之同意始為真實的同意。

5. 預設隱私保護

ePrivacy草案第10條[222]要求電子通訊軟體、網站、搜尋引擎等網路服務，提供使用者隱私設置之選項，避免第三方在使用者之終端設備中儲存訊息或處理已儲存於該終端設備資訊；同時，軟體安

combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 27 determining the information to be presented by the standardized icon and the procedures for providing standardized icons.

[222] U.S., ePrivacy 草案, §10 <Information and options for privacy settings to be provided>

1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end- user or processing information already stored on that equipment.
2. Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.
3. In the case of software which has already been installed on 25 May 2018, the requirements under paragraphs 1 and 2 shall be complied with at the time of the first update of the software, but no later than 25 August 2018.

裝時，應提供使用者有關隱私設定選項之訊息，並經使用者同意方能繼續該安裝程序。

6. 中繼資料處理原則

隱私的保護不僅包括對電子通訊內容的保護，同時還包括對電子通訊中繼資料（Metadata）的保護。中繼資料是指為了傳輸、分配和交互電子通訊內容而在電子通訊網路中處理的資料，包括用來追蹤和確定通訊來源和目的地的資料，在電子通訊服務過程中產生的設備地理位置的資料，以及來電的時間、地點、通話持續的時長等資料。電子通訊涉及到的中繼資料其中不乏與隱私保護息息相關的部分，如果沒有得到使用者的同意，這些資料必須被刪除或者保持匿名，以維護個人隱私。

根據ePrivacy草案第6條規定[223]，電子通訊服務提供者在下列之情況下得處理電子通訊中繼資料：

(1) 為了滿足基於歐盟電子通訊準則指令或歐盟第 2015/212011 號規則，對電子服務提供者對服務品質之強制要求；

(2) 為了計算或交互計算費用、為了發現或制止詐欺或資訊濫用、為了後續訂購之電子通訊服務等目的；

(3) 終端用戶已同意就其中繼資料得使用在一項或多項指定用途

[223] U.S., ePrivacy 草案, §6 <Permitted processing of electronic communications data>

上，包括為了向其提供特定服務，而匿名資訊無法達成該目的或相關目的。

7. 屏蔽來電功能

ePrivacy草案第14條規定[224]，以電話號碼為基礎之人際通訊服務業者應部署最先進的措施以限制不受使用者歡迎的來電，並且也應免費提供受話端使用者封鎖匿名來電以及阻止被自動轉接通話之功能。

8. 行銷規定

根據ePrivacy草案第16條規定[225]，只有在明確地給予用戶免費、

[224] U.S., ePrivacy 草案, §14 <Incoming call blocking>
Providers of publicly available number-based interpersonal communications services shall deploy state of the art measures to limit the reception of unwanted calls by end-users and shall also provide the called end-user with the following possibilities, free of charge:
(a)to block incoming calls from specific numbers or from anonymous sources;
(b)to stop automatic call forwarding by a third party to the end-user's terminal equipment.

[225] Article 16 <Unsolicited communications>
1.Natural or legal persons may use electronic communications services for the purposes of sending direct marketing communications to end-users who are natural persons that have given their consent.
2.Where a natural or legal person obtains electronic contact details for electronic mail from its customer, in the context of the sale of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own similar products or services only if customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection and each time a message is sent.
3.Without prejudice to paragraphs 1 and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall:
(a)present the identity of a line on which they can be contacted; or
(b)present a specific code/or prefix identifying the fact that the call is a marketing call.
4.Notwithstanding paragraph 1, Member States may provide by law that the placing of direct marketing voice-to-voice calls to end-users who are natural persons shall only be allowed in respect of end-users who are natural persons who have not expressed their objection to receiving those communications.
5.Member States shall ensure, in the framework of Union law and applicable national law, that the legitimate interest of end-users that are legal persons with regard to unsolicited communications sent by means set forth under paragraph 1 are sufficiently protected.
6.Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, in an easy

容易拒絕銷售訊息機會的情況下，自然人或法人始得使用其自用戶處取得之電子郵件向用戶直接銷售產品或服務，且每次蒐集資訊時均應給予用戶拒絕行銷之權利。此外透過電子通訊服務直接向終端用戶進行銷售時，應將通訊為銷售性質及該通訊所代表之法人或自然人身分等資訊，告知終端用戶，並應提供必要資訊，使終端用戶得便利撤回其接受進一步銷售訊息的同意。

9. 風險揭露

根據ePrivacy草案第17條規定[226]，電子通訊服務提供者應告知終端用戶可能危及網路或電子通訊服務安全之風險，且於風險超出風險提供者應採取的防護措施之範圍時，應告知終端用戶任何可能的補救措施及該措施可能的花費。

（三）我國個人資料保護法相關規定

我國個人資料保護法並未特別就電子通訊服務或OTT業者訂有特別規定，相較於歐盟GDPR以及2017年提出ePrivacy草案，其針對新型態業者之規範，例如電子通訊服務提供者在使用cookie、IP位址、

manner, to receiving further marketing communications.
7.The Commission shall be empowered to adopt implementing measures in accordance with Article 26(2) specifying the code/or prefix to identify marketing calls, pursuant to point (b) of paragraph 3

[226] U.S., ePrivacy 草案, §17 <Information about detected security risks>
In the case of a particular risk that may compromise the security of networks and electronic communications services, the provider of an electronic communications service shall inform end-users concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, inform end-users of any possible remedies, including an indication of the likely costs involved.

GPS座標等資料時需獲得用戶同意、無論用戶是否同意資料蒐集都必須提供相同的服務等特別規定，都可做為我國未來修法參考方向。以下就數個面向，比較我國個人資料保護法與ePrivacy草案之差異：

1. 行為主體

行為主體上，在我國個人資料保護法於105年修法後，不限行為主體，僅依其組織型態差異區分為公務機關及非公務機關，賦予相異之權利與義務；而GDPR及ePrivacy草案係透過「行為態樣」來做區分，ePrivacy草案特別將電子通訊服務提供者[227]及公開目錄服務業者[228]類型化後，課予額外之義務，以對應其特殊服務態樣以及市場地位，特別是在OTT跨界服務多變的今日，特別針對這兩類業者制定特殊規範，應有其必要性。

2. 保護客體

我國個人資料保護法第2條第1款規定：「自然人之姓名、出生

[227] U.S., ePrivacy 草案, §6、17

[228] U.S., ePrivacy 草案, §15 <Publicly available directories>

1. The providers of publicly available directories shall obtain the consent of end-users who are natural persons to include their personal data in the directory and, consequently, shall obtain consent from these end-users for inclusion of data per category of personal data, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory. Providers shall give end- users who are natural persons the means to verify, correct and delete such data.
2. The providers of a publicly available directory shall inform end-users who are natural persons whose personal data are in the directory of the available search functions of the directory and obtain end-users' consent before enabling such search functions related to their own data.
3. The providers of publicly available directories shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. Providers shall give such end-users that are legal persons the means to verify, correct and delete such data.
4. The possibility for end-users not to be included in a publicly available directory, or to verify, correct and delete any data related to them shall be provided free of charge.

年月日、身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務狀況、社會活動及其他得以直接或間接方式識別該個人之資料。

ePrivacy草案第4條第3項規定：「為符合本規範之目的，下列詞彙之定義應為：

(a) 電子通訊資料係指電子通訊內容及電子通訊中繼資料；

(b) 電子通訊內容係指藉由電子通訊服務交換之內容，例如：文字、語音、影片、圖像、聲音；

(c) 電子通訊中繼資料係指未傳輸、分發或交換電子通訊內容而處理之資料，包含被用來追蹤或辨識通訊來源和位置的資料、提供電子通訊服務所生之設備位置資料及通訊之目的、時間、持續期間與類型。

我國個人資料保護法保護客體係社會生活中足資辨識特定自然人之資訊；而ePrivacy草案之保護客體則不限於乘載有特定自然人資訊之資料，而包括所有電子通訊服務過程中產生之電子通訊中繼資料、電子通訊內容資料及電子通訊資料等，範圍更為明確。

3. 規範行為

我國個人資料保護法准許蒐集、處理、利用之規範則會因係特

殊個資或一般個資、由公務機關或非公務機關處理，而有不同的要件要求，而ePrivacy草案則對每個規範行為再進一步分類。對處理電子通訊資料之行為，區分電子中繼資料、電子通訊資料、電子通訊內容資料；對電子通訊數據之儲存與刪除，則區分為電子通訊內容資訊及電子通訊中繼資訊，對終端設備之保護則區分為使用終端設備儲存及處理能力，蒐集終端設備中軟硬體資訊及對終端設備使用者發布訊息等，分類後則有寬嚴不同的規管方式。

4. 合法依據

依照我國個人資料保護法第6條[229]、第15條[230]以及第19條[231]，

[229] 有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：
一、法律明文規定。
二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
三、當事人自行公開或其他已合法公開之個人資料。
四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

[230] 我國個人資料保護法第 15 條規定：「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：
一、執行法定職務必要範圍內。
二、經當事人同意。
三、對當事人權益無侵害。」

[231] 我國個人資料保護法第 19 條規定：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：
一、法律明文規定。
二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。
三、當事人自行公開或其他已合法公開之個人資料。
四、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經蒐集者依其揭露方式無從識別特定之當事人。
五、經當事人同意。
六、為增進公共利益所必要。
七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護

個人資料處理應有特定目的及法定情形；ePrivacy草案則針對不同資料[232]（電子通訊資料、電子中繼資料、電子通訊內容資料）訂有不同規定，並針對使用者之終設備訂有額外保護規範[233]。

5. 資料安全維護

我國個人資料保護法以機關性質區分，要求公務機關指定專人辦理安全維護事項，而非公務機關要求其應採取適當安全措施；而ePrivacy草案的資安維護要求，原則上是依循GDPR之規定，要求在電子通訊服務提供者在技術或組織上要因應風險提供安全防護措施，另外進一步要求，當電子通訊服務之風險過高時，依ePrivacy第17條[234]電子通訊服務提供者有告知終端用戶有無補救措施和補救措施的花費為何之義務。

（四）結論與建議

ePrivacy草案之保護客體不限於足資識別個人之資訊，而是包括電子通訊服務過程中產生之電子通訊中繼資料以及電子通訊內容資料，且對於網路服務業者使用Cookie追蹤使用者行為有更完整之規範，

之重大利益者，不在此限。
八、對當事人權益無侵害。」

[232] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (OJ L 310, 26.11.2015, p.1–18)

[233] U.S., ePrivacy 草案, §8 <Protection of information stored in and related to end-users' terminal equipment>

[234] U.S., ePrivacy 草案, §17 <Information about detected security risks>

與我國現行隱私保護相關法制有相當程度之不同，二者比較請詳參下表：

圖表 2：ePrivacy 草案與我國法比較

	ePrivacy草案	我國隱私保護相關法制
擴大監管範圍（新型態網路服務）	O	X
秘密通訊保障	O	O （通訊保障監察法[235]）
限制加密	O	O （通訊保障監察法[236]） （但未要求業者設置內部監督機制）
保障使用者行為習慣與設備秘密性	O	X
預設隱私保護	O	X
中繼資料處理原則	O	X
屏蔽來電功能	O	X
行銷規定	O	O （個人資料保護法[237]）
風險揭露	O	X

ePrivacy草案立意良善且規範內容完整，然本團隊審慎研究後，基於以下兩點，建議應先觀察ePrivacy草案未來走向，視其發展情況再決定如何因應：

1. ePrivacy草案仍存在諸多爭議

235 臺灣，通訊保障監察法，第 2 條，「電信事業之通訊監察，除為確保國家安全、維持社會秩序所必要者外，不得為之。前項監察，不得逾越所欲達成目的之必要限度，且應以侵害最少之適當方法為之。」

236 臺灣，通訊保障監察法，第 14 條第 4 項，「通訊系統應具有配合執行監察之功能，並負有協助建置機關建置、維持通訊監察系統之義務。但以符合建置時之科技及經濟上合理性為限，並不得逾越期待可能性。」

237 臺灣，個人資料保護法，第 20 條第 2 項及第 3 項，「非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。」

ePrivacy草案提出至今仍面臨許多爭議，因其規範將嚴重影響數位行銷、即時通訊以及物聯網產業，專家估計若正式施行將對歐洲經濟造成重大影響[238]，除了經濟上的損失，ePrivacy草案對產業也將產生不利影響，以App應用程式開發業為例，倘ePrivacy草案限制App應用程式蒐集使用者資料的範圍，將嚴重衝擊廣告商投放廣告方式以及目前App應用程式自給自足之商業模式，缺少了廣告收益助，App應用程式將無法透過廣告產生收益，進而將開發和營運成本轉嫁到消費者身上，免費App應用程式的數量將會大幅下降[239]。又例如物聯網的領域中，倘機器對機器傳輸亦受其管制，將使裝置間溝通產生延遲，造成效能降低，對該產業發展之影響也有待觀察[240]。以上諸多疑慮也造成ePrivacy草案至今尚未通過。

2. 逾越通傳會業務職掌

ePrivacy草案係規範所有網路服務業者，縱使國家通傳播委員會透過業務職掌法令，規範轄下業者，仍有許多類型網路服務業者（例如：電子商務業者）非國家通傳播委員會所能管轄，無

238 The ePrivacy Regulation: Another Layer of EU Data Regulations, https://www.trendmicro.com/vinfo/us/security/news/online-privacy/the-eprivacy-regulation-another-layer-of-eu-data-regulations
239 深度探索新型態的隱私規範-電子隱私條例：隱私與發展之間的平衡，https://blog.trendmicro.com.tw/?p=55992
240 Why the IoT industry needs to pay attention to ePrivacy Regulation , https://internetofbusiness.com/iot-industry-needs-pay-attention-eprivacy-regulation/

法達到ePrivacy草案一致性規範所有網路服務業者之目的。

二、美國寬頻客戶隱私保護法草案

(一) 概述

美國聯邦通訊委員會（FCC）於 2016 年 4 月 1 日公布一份「制定命令公告（Notice of Proposed Rulemaking）」[241]，針對「寬頻網路接取服務業（Broadband Internet Access Service Provider）」對於客戶的個資與隱私保護提出於美國聯邦法規（Code of Federal Regulations, CFR）第 47 章第 64 部（47 CFR Part 64）新增第 GG 分部（Subpart）的條文草案[242]，並向公眾徵詢意見。以下臚列該草案中的重要內容[243]。

(二) 法規重要內容

1. 定義

(1) 寬頻網路接取服務（Broadband Internet Access Service, BIAS）

草案第 64.7000 條第 c 項採納第 8.2 條第 a 款[244]對「寬頻網路接取服務」之相同定義，即「以有線或無線方式對大眾零售提

[241] 見 http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0401/FCC-16-39A1.pdf，最後到訪為 108 年 11 月 13 日。

[242] US, FCC, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Notice of Proposed Rulemaking, FCC 16-39, April 1, 2016.

[243] 本草案於川普政府上台後已遭否決。

[244] 現為第 8.1 條第 b 款。US, FCC, 47 CFR part 8, Sec8.1(b), “Broadband internet access service is a mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence or that is used to evade the protections set forth in this part.”

供用以向／自所有或幾乎全部網路終端傳輸資料或接收資料之服務，但不包含撥接網路接取服務」[245]。

(2) 客戶（Customer）

草案第 64.7000 條第 e 項將「客戶」定義為「當下或曾經以付費或免費方式使用寬頻網路接取服務的訂戶」及「寬頻網路接取服務的申請者」[246]。

(3) 客戶專屬線路資訊（Customer Proprietary Network Information，CPNI）

草案第 64.7000 條第 g 項對寬頻網路接取服務下的「客戶專屬線路資訊」採納與美國《通訊傳播法（Communication Act）》第 222 條第 h 項第 1 款相同之定義[247]，即「基於業者與客戶之契約關係而自客戶取得與數量、技術組態、類型、目的地、位置及通訊服務的使用總量相關之資訊」，以及「帳單中有關電話轉接服務或長途電話服務有關之資訊」，但不包含「訂戶名單資訊」[248]。

[245] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7000(c), "The term "broadband Internet access services" or "BIAS" has the same meaning given such term in section 8.2(a) of this chapter."

[246] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7000(e), "The term "customer" means:(1) A current or former, paying or non-paying, subscriber to a broadband Internet access service; or (2) An applicant for a broadband Internet access service."

[247] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7000(g), "The term "customer proprietary network information (CPNI)" has the same meaning given to such term in the Communications Act of 1934, as amended, 47 U.S.C. § 222(h)(1)."

[248] US, 47 U.S.C. § 222(h)(1), "The term "customer proprietary network information" means—(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include

FCC 並於公告中舉例[249]，將下列資訊視為寬頻網路接取服務下的「客戶專屬線路資訊」：

A. 服務方案資訊，包含：

a. 服務類別，例如有線網路、光纖網路、行動網路。

b. 服務等級，例如網路速度。

c. 價格。

d. 流量，例如流量限制。

B. 地理位置資訊。

C. 媒體存取控制（Media Access Control，MAC）位址或其他裝置識別碼。

D. 來源與目的地的 IP 位址及網域名稱資訊。

E. 流量數據。

FCC 於公告中另提及下列資訊，並徵詢公眾意見評估是否該列為客戶專屬線路資訊：

A. 通訊埠資訊（Port Information）

作為通訊傳送者或接收者的應用程式之通訊端點，通訊埠號可決定由何應用程式接收通訊。FCC 認為[250]，通訊

subscriber list information."

[249] US, FCC, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Notice of Proposed Rulemaking, FCC 16-39, April 1, 2016, para 41.

[250] US, FCC, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Notice of Proposed Rulemaking, FCC 16-39, April 1, 2016, para 49.

埠號可識別或至少有極高機率可辨識應用程式的種類，進而可辨識該通訊之目的（例如電子郵件或網頁瀏覽）。

因此 FCC 於公告中針對是否將通訊埠資訊（及其他傳輸層協定標頭資訊）視為客戶專屬線路資訊中的「技術組態、類型、目的地」徵詢公眾意見，

B. 應用程式標頭（Application Headers）

應用程式標頭作為協助要求或傳達特定應用程式內容的資料，其功能在於讓終端使用者的裝置及另一端點的對應應用程式得以溝通資訊（例如網頁瀏覽的應用程式標頭通常包含 URL、作業系統及網頁瀏覽器資訊；電子郵件的應用程式標頭通常包含來源與目的地的電子郵件地址）。

FCC 於公告中亦向公眾徵詢是否將應用程式標頭視為客戶專屬線路資訊中的「技術組態、類型、目的地」等資訊[251]。

C. 應用程式使用情形（Application Usage）

FCC 對於是否將業者有意蒐集、儲存的應用程式使用情形（即便與傳播無關）視為客戶專屬線路資訊尚未有定論，因此於公告中一併向公眾徵詢意見[252]。

[251] US, FCC, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Notice of Proposed Rulemaking, FCC 16-39, April 1, 2016, para 50.
[252] US, FCC, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,

D. 客戶居所設備資訊（Customer Premises Equipment Information, CPE Information）

《通訊傳播法》將 CPE 定義為「某人（非業者）於居所內使用於發起（originate）、指示路徑（route）或終止（terminate）電信通訊的設備」[253]，FCC 在公告中舉例，在寬頻服務情境下，CPE 可包含但不限於客戶的智慧型手機、平板電腦、電腦、數據機、路由器、視訊電話、IP 電話等。

FCC 認為[254]，客戶使用的裝置之資訊得以識別其訂購之服務的種類（例如固網或行動上網、有線或光纖網路等），是否將 CPE 資訊視為與客戶之技術組態有關之資訊，或其他符合前述客戶專屬線路資訊類別的資訊，進而受本草案規範，由徵詢公眾意見之必要。

(4) 個人可識別資訊（Personal Identifiable Information，PII）

草案第 64.7000 條第 j 項將「個人可識別資訊」定義為「與特定個人連結或得以連結之任何資訊」[255]，亦即如果該資訊單

Notice of Proposed Rulemaking, FCC 16-39, April 1, 2016, para 51.

[253] US, 47 U.S.C. Sec153(16), "The term "customer premises equipment" means equipment employed on the premises of a person (other than a carrier) to originate, route, or terminate telecommunications."

[254] US, FCC, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Notice of Proposed Rulemaking, FCC 16-39, April 1, 2016, para 52.

[255] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7000(j), "The term "personally identifiable information" or "PII" means any information that is linked or linkable to an individual."

獨或與他資料結合即可識別出特定個人，或該資訊合理的與特定個人的其他資訊有所關聯，則該資訊即屬草案定義的「個人可識別資訊」。

在此定義下，FCC 於公告中舉例，認為「個人可識別資訊」至少包含[256]：姓名、社會安全碼、生日及出生地、母親婚前姓名、政府編給的特別碼（例如駕照號碼、護照號碼、稅籍碼）、住址、電子郵件信箱或其他線上聯絡資訊、電話號碼、媒體存取控制位址或其他裝置識別碼、IP 位址、永久線上識別符（例如獨一的 cookies）、同名或非同名的網路身分、帳戶號碼及其他帳戶資訊（包含登入資訊）、網路瀏覽紀錄、流量數據、行動程式使用資料、當下與過往的地理位置、財務資訊（例如金融帳戶號碼、信用卡或現金卡號碼、信用紀錄）、消費紀錄、醫療與健康資訊、殘疾資訊、生物資訊、教育資訊、受雇資訊、與家庭相關之資訊、種族、信仰、性取向、人口資訊以及可識別屬於個人財產之資訊（例如車牌號碼、裝置序號）。

(5) 客戶專屬資訊（Customer Proprietary Information，Customer PI）

草案第 64.7000 條第 f 項將「客戶專屬資訊」定義包含前述「客戶專屬線路資訊」及寬頻網路接取服務提供者在提供服

[256] US, FCC, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Notice of Proposed Rulemaking, FCC 16-39, April 1, 2016, para 62.

務過程中取得的「個人可識別資訊」[257]。

(6) 客戶聚合資訊（Aggregate Customer PI）

草案第 64.7000 條第 a 項將「客戶聚合資訊」定義為「與一群或一類服務或客戶相關，而已將個別客戶的身分與特徵移除的集合資訊」[258]。

2. 行為規範

(1) 事前告知隱私權政策

依草案第 64.7001 條規範，無論客戶透過親洽、線上、電話中或其他任何方式，業者均須在客戶訂購服務前，向客戶告知隱私權政策[259]，該告知必須：

A. 明確說明並描述[260]：

(a) 提供寬頻網路接取服務所須蒐集客戶專屬資訊之類別。

(b) 業者如何使用，以及在何種情況下將對外揭露何種類別

[257] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7000(f), "The term "customer proprietary information" or "customer PI" means:(1) Customer proprietary network information; and(2) Personally identifiable information (PII) a BIAS provider acquires in connection to its provision of BIAS."

[258] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7000(a), "The terms "aggregate customer proprietary information" or "aggregate customer PI" means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed."

[259] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7001(b)(1), "Notice required under subsection (a) must: (1) Be made available to prospective customers at the point of sale, prior to the purchase of BIAS, whether such purchase is being made in person, online, over the telephone, or via some other means…"

[260] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7001(a)(1), "Specify and describe: (i) The types of customer PI that the BIAS provider collects by virtue of its provision of broadband service; (ii) How the BIAS provider uses, and under what circumstances it discloses, each type of customer PI that it collects; and (iii) The categories of entities that will receive the customer PI from the BIAS provider and the purposes for which the customer PI will be used by each category of entities."

的客戶專屬資訊。

(c) 業者將提供客戶專屬資訊之對象的類別，以及該接受資訊對象使用客戶專屬資訊之目的。

B. 向說明客戶在何種情況下可對專屬資訊行使「選擇退出（Opt-Out）」或「選擇加入（Opt-In）」之權利；並提供客戶簡單而亦於取得之途徑來給予或撤回在寬頻網路接取服務目的之外使用、揭露或供他人存取專屬資訊的同意或撤回同意。該途徑必須持續可用，且客戶無需付出額外成本[261]。

C. 向客戶解釋即便不同意業者在寬頻網路接取服務目的之外使用、揭露或供他人存取專屬資訊，亦不影響客戶訂購服務的履行。但業者也可以清楚且中立的文字說明不同意存取專屬資訊對該客戶的影響[262]。

D. 向客戶說明任何同意（或撤回同意）、拒絕業者在寬頻網路接取服務目的之外使用專屬資訊的意思表示均持續有

[261] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7001(a)(2), "Advise customers of their opt-in and opt-out rights with respect to their own proprietary information, and provide access to a simple, easy-to-access method for customers to provide or withdraw consent to use, disclose, or provide access to customer PI for purposes other than the provision of BIAS. Such method shall be persistently available and made available at no additional cost to the customer."

[262] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7001(a)(3), "Explain that a denial of approval to use, disclose, or permit access to customer PI for purposes other than providing BIAS will not affect the provision of any services to which the customer subscribes. However, the provider may provide a brief description, in clear and neutral language, describing any consequences directly resulting from the lack of access to the customer PI."

效，直到客戶撤銷該次同意或拒絕為止；並向客戶說明有權隨時拒絕或撤銷供他人存取專屬資訊的同意。但業者亦須告知客戶，如有其他法律要求則不在此限[263]。

E. 易於理解且不可誤導[264]。

F. 清晰明確且須使用夠大的字體，同時須置放於客戶明顯可讀的位置[265]。

G. 如將任何部分翻譯為他國語言時，必須完整翻譯[266]。

除此之外，草案亦規範該告知必須經由業者網站首頁之連結、行動裝置應用程式，或其他與網站首頁或應用程式相同功能的管道，對客戶持續揭露[267]。

(2) 隱私權政策重大變更通知

草案參考 FCC 於 2015 年的見解[268]，認定隱私權的重大變

[263] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7001(a)(4), "Explain that any approval, denial, or withdrawal of approval for the use of the customer PI for any purposes other than providing BIAS is valid until the customer affirmatively revokes such approval or denial, and inform the customer of his or her right to deny or withdraw access to such PI at any time. However, the notice must also explain that the provider may be compelled to disclose a customer's PI when such disclosure is provided for by other laws."

[264] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7001(a)(5), "Be comprehensible and not misleading."

[265] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7001(a)(6), "Be clearly legible, use sufficiently large type, and be displayed in an area so as to be readily apparent to the customer…"

[266] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7001(a)(7), "Be completely translated into another language if any portion of the notice is translated into that language."

[267] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7001(b)(2), "Be made persistently available via a link on the BIAS provider's homepage, through the BIAS provider's mobile application, and through any functional equivalent to the provider's homepage or mobile application."

[268] US, FCC, 2015 Open Internet Order, 30 FCC Rcd at 5671-72, para 161, "a "material" change is any change that a reasonable consumer or edge provider would consider important to their decisions on their choice of provider, service, or application."

更指「理性消費者或網路服務／內容提供者（edge provider，非網路接取提供者）將認為對其挑選提供者、服務或應用程式具有重要性的變更」，FCC 同時於公告中對此定義是否需調整或補充向公眾徵詢意見[269]。

依草案第 64.7001 條規範[270]，業者在隱私權政策將有重大變更前，應事先通知既有客戶，該通知必須：

A. 經由「電子郵件或其他雙方同意的電子文件方式」或「客戶的寬頻網路服務帳單」或「業者網站首頁的連結、行動裝置應用程式或其他與網站首頁或應用程式相同功能的管道」，以清楚且顯著的方式向客戶通知[271]。

B. 向客戶以清楚、顯著且易於理解的方式解釋[272]：

[269] US, FCC, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Notice of Proposed Rulemaking, FCC 16-39, April 1, 2016, para 97.

[270] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7001(c), "A BIAS provider must provide existing customers with advanced notice of material changes to the BIAS provider's privacy policies…"

[271] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7001(c)(1), "Be clearly and conspicuously provided through each of the following means: (i) Email or another electronic means of communication agreed upon by the customer and BIAS provider; (ii) On customers' bills for BIAS; and (iii) Via a link on the BIAS provider's homepage, mobile application, and any functional equivalent."

[272] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7001(c)(2), "Provide a clear, conspicuous, and comprehensible explanation of: (i) The changes made to the BIAS provider's privacy policies, including any changes to what customer PI the BIAS provider collects, and how it uses, discloses, or permits access to such information; (ii) The extent to which the customer has a right to disapprove such uses, disclosures, or access to such information and to deny or withdraw access to the customer PI at any time; and (iii) The precise steps the customer must take in order to grant or deny access to the customer PI. The notice must clearly explain that a denial of approval will not affect the provision of any services to which the customer subscribes. However, the provider may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to the customer PI. If accurate, a provider may also explain in the notice that the customer's approval to use the customer's PI may enhance the provider's ability to offer products and services tailored to the customer's needs."

(a) 隱私權政策變更之處，包含業者蒐集的客戶專屬資訊的變更，以及業者使用、揭露或供他人存取該資訊的方式之變更。

(b) 客戶在何種程度內有權拒絕前述變更後的使用、揭露或供他人存取，以及有權在任何時間拒絕或撤銷對於存取專屬資訊之同意。

(c) 客戶欲允許或拒絕存取專屬資訊之具體步驟。該通知必須明確讓客戶知悉任何拒絕之意均不影響客戶已訂購之服務。但業者也可以清楚且中立的文字說明不同意存取專屬資訊對該客戶的影響。如與實情相符，業者亦可向客戶說明如客戶允許使用專屬資訊，將可優化業者對客戶提供更多的精準行銷。

C. 向客戶說明任何同意或拒絕業者對於寬頻網路接取服務目的之外使用專屬資訊的行為均持續有效，直到客戶撤銷該次同意或拒絕為止[273]。

D. 易於理解且不可誤導[274]。

E. 清晰明確且須使用夠大的字體，同時須置放於客戶明顯可

[273] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7001(c)(3), "Explain that any approval or denial of approval for the use of customer PI for purposes other than providing BIAS is valid until the customer affirmatively revokes such approval or denial."

[274] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7001(c)(4), "Be comprehensible and not misleading."

讀的位置[275]。

F. 如將任何部分翻譯為他國語言時，須將全部通知內容翻譯為他國語言[276]。

(3) 利用客戶專屬資訊之要件

草案第 64.7002 條將業者利用客戶專屬資訊之行為區分不同類型，分別規範其合法要件：

A. 視為當事人同意

依草案規範[277]，下列情形（目的）視為客戶已同意業者使用、揭露或供他人存取客戶專屬資訊：

(a) 提供寬頻網路接取服務而取得（衍生取得）之資訊，或為提供服務所必要取得或使用之資訊。

(b) 為寬頻網路接取服務之提供、租用、收費而蒐集資訊，

[275] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7001(c)(5), "Be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to customers."

[276] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7001(c)(6), "Have all portions of the notice translated into another language if any portion of a notice is translated into that language."

[277] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7002(a), "A customer is considered to have provided approval for the customer's BIAS provider to use, disclose, or permit access to customer PI for the following purposes:(1)In its provision of the broadband Internet access service from which such information is derived, or in its provision of services necessary to, or used in, the provision of such broadband service.(2)To initiate, render, bill and collect for broadband Internet access service, and closely related services, e.g., tech support related to the broadband Internet access services.(3)To protect the rights or property of the BIAS provider, or to protect users of the broadband Internet access service and other BIAS providers from fraudulent, abusive, or unlawful use of the broadband Internet access service.(4)To provide any inbound marketing, referral, or administrative services to the customer for the duration of the interaction, if such interaction was initiated by the customer and the customer approves of the use of such information to provide such service.(5)To support queries by Public Safety Answering Points and other authorized emergency personnel pursuant to the full range of NG911 calling alternatives (including voice, text, video and data); to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency. (6)As otherwise required by law."

並與該服務密切相關，例如寬頻網路接取服務的技術支援等。

(c) 為保護業者的權利或財產，或為保護寬頻網路接取服務使用者或其他寬頻網路接取服務提供者免於詐欺、誹謗、或其他不法利用寬頻網路服務之行為。

(d) 基於客戶主動要求並同意使用客戶專屬資訊的行銷（inbound marketing）、推薦或行政服務。

(e) 為避免客戶受到生命、身體等損害之緊急情況所須對有關單位或人員提供資訊。

(f) 其他法律要求。

B. 無需當事人同意

依草案規範[278]，如客戶已向業者訂購某類服務（例如固網或行動上網），則業者可基於「行銷與該類服務相同的其他服務」之目的利用客戶專屬資訊。

C. 選擇退出或選擇加入之同意

依草案規範[279]，在下列情況時，業者須取得客戶的「選

[278] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7002(b), "A BIAS provider may use customer PI for the purpose of marketing additional BIAS offerings in the same category of service (e.g., fixed or mobile BIAS) to the customer, when the customer already subscribes to that category of service from the same provider, without further customer approval."

[279] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7002(e), "Except as otherwise provided in subsection (a), a BIAS provider must obtain opt-out or opt-in approval from a customer to: (1)Use customer PI for the purpose of marketing communications-related services to that customer; and (2)Disclose or permit access to customer PI to its affiliates that provide communications-related services for the purpose of marketing communications-related services to that customer."

擇退出（Opt-Out）」或「選擇加入（Opt-In）」之同意，始可利用客戶專屬資訊：

(a) 利用客戶專屬資訊向該客戶行銷「與通訊業務相關之服務」。

(b) 基於「行銷與通訊業務相關之服務」的目的，向提供該相關服務之關係企業揭露或供其存取客戶專屬資訊。

D. 選擇加入之同意

依草案規範[280]，除前述「視為同意」、「無需同意」及「由業者自行決定採『選擇退出』或『選擇加入』之同意」等情形外，業者於其他情況欲使用、揭露或供他人存取客戶專屬資訊時，均須事先取得客戶「選擇加入」之同意。

E. 同意之方式

依草案規範[281]，業者須提供客戶簡單且易於取得之途徑以隨時給予或撤銷同意，而該方式必須向客戶明確揭露並持續可得，且客戶無須付出額外成本。又客戶向業者表達其同意或撤銷同意之意思後，應立即生效。

[280] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7002(f), "Except as otherwise provided, a BIAS provider must obtain customer opt-in approval to use, disclose, or permit access to customer PI."

[281] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7002(d), "A BIAS provider must make available a simple, easy-to-access method for customers to provide or withdraw consent at any time. Such method must be clearly disclosed, persistently available, and made available at no additional cost to the customer. The customer's action must be given effect promptly after the decision to provide or withdraw consent is communicated to the BIAS provider."

F. 告知後同意（知情同意）

依草案規範[282]，有效的「選擇退出」或「選擇加入」之同意以業者於事前「清楚且顯著告知必要資訊」為前提，告知內容包含：

(a) 業者尋求客戶同意使用、揭露或供他人存取之客戶專屬資訊的類別。

(b) 使用客戶專屬資訊之目的。

(c) 業者欲揭露或供存取客戶專屬資訊之對象或其類別。

G. 使用與揭露客戶聚合資訊

依草案規範[283]，在符合下列條件時，業者可在提供寬頻網路接取服務的目的之外使用、揭露或供他人存取客戶的聚合資訊，但須由業者負擔該聚合資訊中的客戶身分與特徵已被移除的舉證之責：

[282] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7002(c), "Except as described in subsection (a) of this section, a BIAS provider must solicit customer approval, as provided for in subsections (e) and (f) of this section, when it intends to first use, disclose, or provide access to the customer's proprietary information and in so doing must clearly and conspicuously disclose:(1)The types of customer PI for which it is seeking customer approval to use, disclose or permit access to; (2)The purposes for which such customer PI will be used; and (3)The entities or types of entities to which it intends to disclose or provide access to such customer PI."

[283] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7002(g), "A BIAS provider may use, disclose, and permit access to aggregate customer PI other than for the purpose of providing BIAS and for services necessary to, or used in, the provision of BIAS, if the BIAS provider:(1)Determines that the aggregated customer PI is not reasonably linkable to a specific individual;(2)Publicly commits to maintain and use the aggregate customer PI in a non-individually identifiable fashion and to not attempt to re-identify such information;(3)Contractually prohibits any entity to which it discloses or permits access to the aggregate customer PI from attempting to re-identify such information; and(4)Exercises reasonable monitoring to ensure that those contracts are not violated.
For purposes of this section, the burden of proving that individual customer identities and characteristics have been removed from aggregate customer PI rests with the BIAS provider."

(a) 確認該客戶聚合資訊無法以合理方式與特定個人連結。

(b) 公開承諾保持並以不具個人識別性的方式使用客戶聚合資訊，並承諾不以任何方式再識別該資訊。

(c) 以契約方式禁止揭露或供存取客戶聚合資訊的對象以任何方式再識別該資訊。

(d) 以合理監督方式確保無人違反該契約。

(4) 同意合規性紀錄

草案第 64.7003 條規定，業者必須導入足以於事前及事後清楚確認客戶同意使用、揭露及供他人存取客戶專屬資訊的機制[284]，業者應：

A. 訓練員工知悉何時獲得及何時未獲得授權使用、揭露或供他人存取客戶專屬資訊，且應訂定明確的獎懲程序[285]。

B. 維護一份至少包含一年內將客戶專屬資訊揭露予或供第三人存取之紀錄。該紀錄應包含揭露予或供第三人存取之客戶專屬資訊的具體描述、接收客戶專屬資訊之第三人的具體清單，以及揭露予或供第三人存取該資訊的依據[286]。

[284] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7003, "A BIAS provider must implement a system by which the status of a customer's approval to use, disclose, and provide access to customer PI can be clearly established both prior to and after its use, disclosure, or access…"

[285] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7003(a), "Train its personnel as to when they are and are not authorized to use, disclose, or permit access to customer PI and have an express disciplinary process in place."

[286] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7003(b), "Maintain a record of all instances where customer PI was disclosed to or accessed by third parties for at least one year. The record must include a description of the specific customer PI that was disclosed to or accessed by third

C. 維護一份至少包含一年內所有向客戶作成之通知的紀錄，無論該通知是以口頭、書面或電子方式為之[287]。

D. 建立關於業者遵循本分部規範的監督審查程序[288]。

E. 在知悉「選擇退出」機制無法適當發揮作用（客戶無法選擇退出一事並非特例）的 5 日內，或在知悉業者於「選擇加入」的情境下，未先得到客戶選擇加入之同意便使用、揭露或供他人存取客戶專屬資訊的 5 日內，以書面向 FCC 通報該情形。即便業者向客戶提供其他選擇退出的方式，亦不解免前述通報義務[289]。此通報應包含：

(a) 業者名稱。

(b) 系爭選擇退出機制的描述及相關範圍內發生的問題。

(c) 描述下列事項：

i. 違反選擇退出或選擇加入規定而使用、揭露或存取的

parties, a list of the specific third parties who received the customer PI, and the basis for disclosing or providing access to such information to third parties."

[287] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7003(c), "Maintain a record of all customer notifications, whether oral, written, or electronic, for at least one year."

[288] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7003(d), "Establish a supervisory review process regarding the provider's compliance with the rules in this subpart."

[289] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7003(e), "Provide written notice to the Commission within five days of the discovery of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly; or the provider used, disclosed, or permitted access to customer PI subject to opt-in approval requirements without first having received opt-in approval. Such notice must be submitted even if the provider offers other methods by which customers may opt-out. The notice shall include:(1)The provider's name;(2)A description of the opt-out mechanism(s) at issue and the problem(s) experienced, if relevant;(3)A description of:(i)Any customer PI used, disclosed, or accessed without opt-out or opt-in approval;(ii) With whom or by whom such customer PI has been used, disclosed, or accessed;(iii)For what purposes such customer PI was used, disclosed, or accessed; and (iv)Over what period of time such customer PI was used, disclosed, or accessed;(4)The remedy proposed and when it will be or was implemented; and(5)A copy of the notice provided contemporaneously to customers."

任何客戶專屬資訊。

ii. 何人使用、揭露或存取該客戶專屬資訊。

iii. 為何目的而使用、揭露或存取該客戶專屬資訊。

iv. 該客戶專屬資訊在何段期間內遭使用、揭露或存取。

(d) 矯正措施及導入時間。

(e) 同時提供給客戶的通報影本。

(5) 安全維護責任

草案第 64.7005 條要求業者確保所接收、維護、使用、揭露或供他人存取之客戶專屬資訊的安全性、機密性及完整性，避免任何未獲授權之使用或揭露，或超出授權範圍的使用，至少應符合下列要求[290]：

A. 建置並執行例行性的風險管理評估，並即時因應任何經由該評估而識別出的資料安全系統弱點。

B. 對需要處理客戶專屬資訊之受雇人、承商及關係企業（人員）辦理資料安全程序的教育訓練。

[290] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7005(a), "A BIAS provider must ensure the security, confidentiality, and integrity of all customer PI the BIAS provider receives, maintains, uses, discloses, or permits access to from any unauthorized uses or disclosures, or uses exceeding authorization. At minimum, this requires a BIAS provider to:(1)Establish and perform regular risk management assessments and promptly address any weaknesses in the provider's data security system identified by such assessments;(2)Train employees, contractors, and affiliates that handle customer PI about the BIAS provider's data security procedures;(3)Designate a senior management official with responsibility for implementing and maintaining the broadband provider's information security measures;(4)Establish and use robust customer authentication procedures to grant customers or their designees' access to customer PI; and(5)Notify customers of account changes, including attempts to access customer PI, in order to protect against fraudulent authentication."

C. 指派高階管理人負責導入並維護資訊安全措施。

D. 在提供客戶或其受託人存取客戶專屬資訊時，建置並採用健全的客戶驗證程序。

E. 向客戶通知帳戶變更事宜，包含存取客戶專屬資訊的嘗試，以避免驗證詐欺。

草案並規定[291]，業者可採取任何足以合理滿足上列要求的安全措施，並至少應考量：

A. 業者業務的性質與範圍。

B. 業者保有的客戶專屬資訊之敏感性。

(6) 事故通報

草案第 64.7006 條課予業者通報（知）侵害事故的義務，依受通報對象區分如下：

A. 向客戶通知

依草案規定[292]，業者依執法需求，應至遲於發現侵害後 10 日內，向客戶專屬資訊受該侵害影響的客戶為事故

[291] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7005(b), "A BIAS provider may employ any security measures that allow the provider to reasonably implement the requirements set forth in this section, and in doing so must take into account, at minimum,:(1)The nature and scope of the BIAS provider's activities;(2)The sensitivity of the customer proprietary information held by the BIAS provider."

[292] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7006(a), "A BIAS provider must notify affected customers of covered breaches of customer PI no later than 10 days after the discovery of the breach, subject to law enforcement needs."

通知，通知方式可擇一採[293]：

(a) 書面通知寄送客戶提供用於聯繫的收件地址。

(b) 電子郵件寄送，或以客戶提供用於通知侵害事故的其他電子方式。

向客戶通知的內容應包含[294]：

(a) 安全侵害的日期、預估日期或預估期間。

(b) 對遭到未經授權或逾越授權範圍而使用、揭露、存取或合理相信遭使用、揭露或存取的客戶專屬資訊的描述。

客戶可用以聯繫業者以查詢安全侵害及業者保有關於該客戶的客戶專屬資訊之聯絡方式。

(a) FCC 及任何與客戶或該服務相關的州立監管機關之聯絡資訊。

[293] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7006(a)(1), "A BIAS provider required to provide notification to a customer under this subsection may provide such notice by any of the following methods:(i)Written notification, sent to the postal address of the customer provided by the customer for contacting that customer; or (ii)Email or other electronic means using information provided by the customer for contacting that customer for data breach notification purposes."

[294] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7006(a)(2), "The customer notification required to be provided under this section must include:(i)The date, estimated date, or estimated date range of the breach of security;(ii)A description of the customer PI that was used, disclosed, or accessed, or reasonably believed to have been used, disclosed, or accessed, by a person without or exceeding authorization as a part of the breach of security;(iii)Information that the customer can use to contact the BIAS provider to inquire about the breach of security and the customer PI that the BIAS provider maintains about that customer; (iv)Information about how to contact the Federal Communications Commission and any state regulatory agencies relevant to the customer and the service; and(v)Information about the national credit-reporting agencies and the steps customers can take to guard against identity theft, including any credit monitoring or reporting the telecommunications carrier is offering customers affected by the breach of security."

(b) 國家信用報告機構的資訊，以及客戶可採取用以避免身分竊盜的步驟，包含業者提供受安全侵害影響之客戶的任何信用監控或通報機制。

但草案亦規定[295]，如聯邦執法機構認為前述通知將阻礙犯罪或國家安全事件的調查時，亦可以書面要求業者在合理必要的期限內延後該通知。該聯邦執法機構亦可嗣後以書面撤銷延期的要求，或在其認為有必要的期限內要求再次延後通知。

B. 向 FCC 通報

依草案規定[296]，業者應至遲於發現任何客戶專屬資訊之侵害後 7 日內，以 FCC 的網站上用以通報侵害的通報系統，以電子方式將侵害通報 FCC。

C. 向聯邦執法機構通報

依草案規定[297]，業者如合理相信客戶專屬資訊受侵害

[295] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7006(a)(3), "If a federal law enforcement agency determines that the notification to customers required under this subsection would interfere with a criminal or national security investigation, such notification shall be delayed upon the written request of the law enforcement agency for any period which the law enforcement agency determines is reasonably necessary. A law enforcement agency may, by a subsequent written request, revoke such delay or extend the period set forth in the original request made under this subparagraph by a subsequent request if the law enforcement agency determines that further delay is necessary."

[296] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7006(b), "A BIAS provider must notify the Federal Communications Commission of any breach of customer PI no later than seven days after discovering such breach. Such notification shall be made electronically by means of a reporting system that the Commission makes available on its website."

[297] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7006(c), "A BIAS provider must notify the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (Secret Service) whenever a breach is reasonably believed to have compromised the customer PI of more than 5,000 customers, no later than seven (7) days after discovery of the breach, and at least three (3) days before notification

事故影響的客戶人數逾 5000 人時，應至遲於發現侵害後 7 日內，或在通知客戶至少 3 天前（以先屆至者為準），以 FCC 於網站上提供連結的中央通報機制，將侵害通報聯邦調查局（FBI）及美國特勤局（Secret Service）。

此外，草案課予業者保存通報紀錄的義務[298]，要求業者須將任何發現的安全侵害及通知客戶、通報 FCC、聯邦調查局和特勤局的資訊作成紀錄並保存至少 2 年，該紀錄在可行的範圍內必須包含「發現侵害及通報的日期」、「受侵害影響的客戶專屬資訊的詳細描述」以及「該侵害的具體情狀」。

(三) 我國法規比較

相較之下，由於我國以一部個人資料保護法作為所有公務機關與非公務機關在個人資料保護方面的管制基本法，因此在規管寬頻網路接取服務的相關法律（例如《電信法》或 108 年 6 月 26 日公布之《電信管理法》）中，未對受規範的個人資料另為規定，也未特別對於業者的行為規範（尤其是利用客戶資料的要件類型）有所著墨。以下臚列數項重要差異：

to the affected customers, whichever comes first. Such notification shall be made through a central reporting facility. The Commission will maintain a link to the reporting facility on its website."

[298] US, FCC, 47 CFR part 64, Proposed Rules, April 1, 2016, Sec64.7006(d), "A BIAS provider must maintain a record of any breaches of security discovered and notifications made to customers, the Commission, the FBI, and the Secret Service pursuant to this section. The record must include, if available, dates of discovery and notification, a detailed description of the customer PI that was the subject of the breach, and the circumstances of the breach. BIAS providers shall retain such records for a minimum of 2 years."

1. 受保護主體

我國個人資料保護法所保護者為現生存之自然人[299]，《電信法》雖保障「用戶」之權益，卻未對「用戶」一詞有具體定義，但《電信管理法》第 3 條第 1 項第 9 款則將「用戶」定義為「因電信服務之使用，與電信事業發生服務契約關係之相對人」。

相較之下，FCC 之草案所欲保護的對象明確包含「當下或曾經使用寬頻網路接取服務的訂戶」及「寬頻網路接取服務的申請者」，將訂戶於事前、事中及事後（的個人資料）均納入保護範圍。

然由於目前《電信法》或《電信管理法》均不具體規範個人資料之合規要件，因此就用戶個人資料的保障仍回歸適用個人資料保護法，而依上揭定義，個人資料保護法保護之範圍當包含（現生存的）申請服務、使用服務及已不再使用服務之用戶，是以此處差異應不致構成保護密度的落差。

2. 受保護客體

我國個人資料保護法所保護之個人資料指「自然人之姓名、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

[299] 我國，個人資料保護法施行細則，第 2 條：「本法所稱個人，指現生存之自然人」。

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」[300]，採例示立法模式將得以直接或間接方式識別[301]特定自然人之資料均納入保護。

然而所稱「得以直接或間接方式識別」之判斷，於實務操作上迭有爭議，或時有個人資料保護法主管機關認為須「從蒐集者本身綜觀各種情況與事證加以判斷，原無一致性標準」之情事[302]，無論對當事人的保護或蒐集機關的法遵要求均易產生模糊之處。

且個人資料保護法既適用於各領域事業，似難期待個人資料保護法主管機關針對各行業涉及之細項資料逐一解釋是否屬於我國個人資料保護法所欲保護之個人資料。

相較之下，FCC 之草案定義受保護的「客戶專屬資訊」包含「客戶專屬線路資訊」及「個人可識別資訊」，再於公告中明確例舉 FCC 所欲保護的資訊類型，此規管方式對於中央目的事業主管機關而言，應較能有施力空間。

3. 事前告知法定資訊

300 我國，個人資料保護法，第 2 條第 1 款。

301 我國，個人資料保護法施行細則，第 3 條：「本法第二條第一款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」。

302 例如法務部法律決字第 10303506790 號書函，103 年 6 月 18 日，「…查行動電話是否得以直接或間接方式識別者，需從蒐集者本身綜觀各種情況與事證加以判斷，原無一致性之標準，此宜於個案中加以審認（個人資料保護法施行細則第 3 條立法理由參照），尚未可僅依單一資料類型，即遽論是否為個人資料保護法所稱之個人資料」。

我國個人資料保護法第 8 條[303]及第 9 條[304]課予蒐集機關向當事人揭露法定資訊之義務，此與 FCC 之草案第 64.7001 條的規範意旨相同，均是為滿足「公開透明」的（個人資料保護）普世原則。

但由於我國個人資料保護法並未對「撤回同意」定有明文，因此並未如同 FCC 之草案要求將撤回同意之權利及方式納入應揭露的法定資訊。此外，對於法定資訊揭露方式（例如：文字須易於理解且不可誤導、字體須夠大、呈現位置須明確等）亦未於條文中設有規定。

考量法定資訊的揭露對象為當事人（用戶），如未特別要求業者揭露法定資訊的形式要件，恐造成業者使用艱澀難解之法律文字撰寫法定資訊，再以不夠明確方式向當事人提出，進而造成當事人無法或難以理解該資訊內容之憾事。因此是否對法定資訊的形式要件特別訂定規範，應有評估之必要。

4. 重大變更通知

我國個人資料保護法未如 FCC 之草案明文課予蒐集機關在

303 我國，個人資料保護法，第 8 條第 1 項：「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、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」。

304 我國，個人資料保護法，第 9 條第 1 項：「公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項」。

法定應揭露資訊遇有重大變更時，應在事前通知當事人之義務，或將造成當事人（用戶）不知業者對其個人資料將有其他利用方式，恐易生爭議。

5. 利用個人資料之要件

我國個人資料保護法針對非公務機關利用個人資料之合法要件規定於第 20 條第 1 項[305]，原則上僅能於蒐集目的之必要範圍內利用，特定條件下始有例外（例如取得當事人同意）。

然而，各業者於實務上對於何種利用行為屬於「履行契約之目的必要範圍」或「須另行符合例外始得為之的目的外利用」屢見爭議，尤其在行銷之商品或服務方面，應如何判斷是否屬於蒐集目的內利用實為業者關注之焦點。

相較之下，FCC 之草案具體區分各種類型的利用個人資料行為，並分別於條文中指明是否需要及如何取得「當事人之同意」，此規管方式應更可讓受規範之業者有所依循。

值得留意的是，我國個人資料保護法對於在蒐集目的外利用個人資料的同意規範並無「選擇退出」及「選擇加入」的形式區

[305] 我國，個人資料保護法，第 20 條第 1 項：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為增進公共利益所必要。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、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經蒐集者依其揭露方式無從識別特定之當事人。六、經當事人同意。七、有利於當事人權益」。

分，第 7 條第 2 項規定「第十六條第七款、第二十條第一項第六款所稱同意，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示」，即指當事人應有一積極行為（單獨所為）表達同意之意思。

6. 聚合資料使用

我國個人資料保護法中並無「聚合資料／訊（Aggregate Data／Information）」一詞，但依個人資料保護法主管機關之見，如個人資料去識別後之呈現方式以無從直接或間接識別特定個人，便不再屬於個人資料，蒐集機關利用去識別之資料即不受個人資料保護法拘束[306]。此「去識別資料」性質應與 FCC 之草案所稱「聚合資訊」相似。

然而，個人資料去識別化之最大隱憂與爭議在於「去識別之程度」，或謂「再識別的可能」，因此，FCC 之草案採取「課予業者舉證聚合資訊中的客戶身分與特徵已被移除之責」、「要求業者承諾不以任何方式再識別該資訊，並以契約禁止取得聚合資訊之對象以任何方式再識別該資訊」等規管措施，值得我國參考。

[306] 法務部，103 年 11 月 17 日，法律字第 10303513040 號函釋（節錄），「…如將公務機關保有的個人資料處理技術去識別化而呈現方式已無從直接或間接識別特定個人，即非屬個人資料，自非個人資料保護法之適用範圍…」。

(四) 監理措施分析

在我國對於個人資料保護的法律架構尚未變動的前提下(即以一部個人資料保護法作為基本法，有專責解釋主管機關，但由各中央目的事業主管機關職司該法的事實認定及執法)，國家通訊傳播委員會（以下稱「通傳會」）作為寬頻網路接取服務（電信服務）事業的中央目的事業主管機關，在監理措施上可有下列方案選項，以下說明優劣：

1. 提出修正個人資料保護法條文草案

我國以一部個人資料保護法作為保護個人資料之基本法，此與美國不同，因此將涉及個人資料行為要件之規範提由該法主管機關參考修正，應最能達成規管上的一致性。

然而，立法程序有其繁瑣之處並時易延宕，通傳會難以掌握個人資料保護法主管機關推動修法之進度，亦難評估立法機關通過修正之時程；且本研究以 FCC 之草案提出重要參考修正之處，多有高度領域（電信事業）特性，是否適合於個人資料保護法中明訂讓各領域事業一併適用，應仍有斟酌餘地。

2. 於《電信管理法》新增條文

由於我國個人資料保護法為基本法，即特別法律如有特殊規範便優先適用。據此，通傳會應可考量於即將生效之《電信

管理法》新增條文，針對電信用戶之個人資料保護訂定特別要求，無特殊規範需求之處則回歸適用個人資料保護法。

在此措施下，通傳會可於《電信管理法》新增「電信用戶資料保護」章節，明確定義「受保護的電信用戶及受保護之資料範圍」、「電信事業應向電信用戶揭露的法定資訊實質內容與形式要件」、「法定應揭露資訊內容重大變更的通知義務」、「何種利用資料之行為視為或無須另取得用戶同意」、「何種利用資料之行為須如何取得用戶之同意（選擇退出或選擇加入）」、「電信事業的記錄與舉證責任」等。此方式應可令通傳會更能發揮中央目的事業主管機關的監理功能，且對涉及電信用戶資料的行為規範不再仰賴個人資料保護法主管機關之解釋，將更有執法空間。

然而，如獨立將電信用戶資料之行為規範納入特別法管轄，通傳會即需確保配置足夠能量對特別法之規範作成解釋，並據以執法；此外，我國個人資料保護法主管機關刻正啟動法規調整程序以向歐盟爭取跨境傳輸資料的適足性認定，未來的規管措施似朝「專責主管機關」方向發展，即由單一主管機關作為個人資料保護法的解釋與執法機關[307]，則若通傳會將來不

[307] 潘姿羽，台歐 27 日再啟 GDPR 協商 修個人資料保護法勢在必行，中央通訊社，2019 年 11 月 26 日，https://www.cna.com.tw/news/afe/201911260119.aspx，最後到訪為 108 年 11 月 29 日。

再是個人資料保護法中的（中央目的事業）主管機關，卻另有主管的特別法針對電信用戶資料之行為訂定規範，此雙頭併行的監理方式是否妥當，似有充份評估必要。

3. 修正《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》

在法律修正之外，通傳會亦可修正現行依個人資料保護法第 27 條第 2 項及第 3 項的授權[308]訂定之《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》（以下稱「該辦法」），逕將新增條文置入該辦法中。

然而，由個人資料保護法第 27 條第 1 項「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏」之規定來看，該條所欲針對者乃非公務機關對於個人資料檔案的「安全」措施（避免個人資料被竊取、竄改、毀損、滅失或洩漏之措施），但本研究參考 FCC 之草案提出的修正參考多為「行為規範」，係對業者的行為要件制定遵循義務，若將此納入該辦法中，恐有超出母法授權之虞，易生爭議。

[308] 我國，個人資料保護法，第 27 條第 2 項：「中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法」；第 3 項：「前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之」。

4. 以行政指導方式統一業界標準

最後，如不採取法律或法規命令的修正方式，則通傳會仍有《行政程序法》中的「行政指導」[309]可作為監理手段。

然而，一來行政指導並不具法律上強制力，業者（相對人）可任意拒絕[310]；二來行政指導所欲輔導、建議業者遵循者仍以現行有效法律為標的，若未（依本研究參考 FCC 之草案提出的修正）變動任何法律，則縱使通傳會發動行政指導，亦不能逾越現行法律規範。

(五) 建議方向

綜上所述，本研究認為通傳會應可待「本次個人資料保護法之修正是否將該法的解釋與執法權歸由單一專責主管機關負責」一事明朗後，再行決定是否啟動修法工程。但在此之前，通傳會仍可為下列作為：

1、 對業者就「行銷範圍」及「法定資訊揭露內容」、「須取得同意之利用目的」為行政指導

我國個人資料保護法第 20 條第 1 項規範非公務機關利用個人資料之行為必須與蒐集之目的相符，第 8 條第 1 項第 2 款

309 我國，行政程序法，第 165 條：「本法所稱行政指導，謂行政機關在其職權或所掌事務範圍內，為實現一定之行政目的，以輔導、協助、勸告、建議或其他不具法律上強制力之方法，促請特定人為一定作為或不作為之行為」。

310 我國，行政程序法，第 166 條第 2 項：「相對人明確拒絕指導時，行政機關應即停止，並不得據此對相對人為不利之處置」。

亦規定非公務機關應於事前向當事人明確告知「蒐集個人資料之目的」。

在此前提下，由於業者關注焦點之一在於「可向用戶行銷商品或服務之範圍」，因此通傳會應可參考 FCC 之草案，以行政指導方式向業者表明通傳會之立場（仍需充分辯論並適時徵詢利害關係人意見），例如：

(1) 業者向用戶行銷與其訂購之服務屬同類型的商品或服務時（例如用戶申辦行動寬頻服務，業者對其行銷行動寬頻優惠方案），屬於蒐集目的內之利用個人資料行為。

(2) 業者向用戶行銷與其訂購之服務不屬同類型的商品或服務時（例如用戶申辦行動寬頻服務，業者對其行銷固定通信服務），屬於蒐集目的內利用個人資料之行為，但應提供用戶單獨針對此行銷內容表示拒絕。

(3) 業者向用戶行銷第三方企業的商品或服務時，屬於蒐集目的外利用個人資料之行為，須另滿足其他合法要件（例如取得用戶同意）

2、 備妥「電信用戶資料保護」具體內容

又即便未來我國以單一專責主管機關職司個人資料保護法之解釋與執法，該專責主管機關（至少在初期）對於各事業

之特性必難以確實掌握，極有可能須仰賴各中央目的事業主管機關針對產業性質提出該領域個人資料保護的重要焦點，以利該專責主管機關憑藉作為執法依據，甚至頒布產業實務指引促成各事業的法律遵循。

因此，即便通傳會或無修法需求，但預先備妥符合監理事業特性的用戶資料保護具體規範，即可適時提供專責主管機關作為參考。