「強化數位隱私保障所涉個人資料保護法相關議題研析」委託研究計畫

結案報告

委託機關：國家發展委員會

受託單位：達文西個資暨高科技法律事務所

中華民國 110 年 11 月

「強化數位隱私保障所涉個人資料保護法相關議題研析」委託研究計畫

結案報告

受託單位：達文西個資暨高科技法律事務所

計畫主持人：葉奇鑫

計畫期程：中華民國 110 年 4 月至 110 年 11 月

國家發展委員會 委託研究

中華民國 110 年 11 月

中文摘要

鑑於國際間因應新興科技對個資保護之衝擊，陸續檢討該國之個人資料保護法相關規定，為與國際接軌，我國亦持續檢討國內個人資料保護法（以下稱個資法）之相關規定，俾使我國個資法對民眾個資之保護程度與先進國家相當；同時，行政院於 110 年 1 月啟動之「臺灣開放政府國家行動方案」的「強化數位隱私與個資保護」承諾事項，以及刻正研議之「國家人權行動計畫」子議題，均將個資法特定規範之修正納入檢討。

據此，本研究即就(1)當事人拒絕權；(2)當事人查閱權；(3)告知目的外利用個資或利用開放資料為自動化決策；(4)個資事故通知；(5)當事人同意；(6) 個資衝擊影響評估；(7)個資保護官等七項議題，比較現行個資法與歐、美、日、韓、新加坡等國之法規差異，提出相關法規（個資法與其施行細則）增修條文草案建議，並擬訂關於(1)拒絕行銷；(2)網路活動查閱權；(3)個資侵害事故通知；(4)個資保護影響評估等四份指引草案供機關參考，期在「強化個資保護」的同時，亦能兼顧「個人資料的合理運用」。

Abstract

Countries around the world are all looking to update their data protection legislation to address the impacts of new technologies on data protection. No exception to this international trend, Taiwan has also been reviewing the provisions of its Personal Data Protection Act (PDPA), so as to ensure a consistent level of protection under the PDPA with the laws of other major countries. In the meantime, the commitment by the Executive Yuan to "Strengthen Digital Privacy and Personal Data Protection", as a part of the Open Government National Action Plan launched in January 2021, together with the National Human Rights Action Plan currently under development, have both highlighted considerations on the potential amendment to the PDPA.

In light of the above, this research project compares and analyzes provisions of the PDPA and the data protection laws of the EU, the U.S., Japan, South Korea and Singapore, with regard to the following 7 topics: (1) the data subject's right to object; (2) the data subject's right of access; (3) information obligation in cases of using data for a purpose other than that of collection or using open data; (4) data breach notification; (5) the data subject's consent; (6) data protection impact assessment and (7) data protection officer. On basis of the foregoing, and in an effort to balance "strengthened data protection" with "appropriate use of personal data", this research project proposes amendments to the relevant legislation (the PDPA and its enforcement rules), as well as 4 draft guidelines for reference by organizations, respectively on (1) objection to direct marketing; (2) right of access for internet activity personal data; (3) data breach notification and (4) data protection impact assessment.

目錄

表目錄

第一章　研究目的

隨著數位時代所面臨之新興議題，人民對個資保護之意識逐漸提升，如何強化個資保護與兼顧個資合理運用，已成為各國政府面對之重要課題。

鑑於國際間因應新興科技對個資保護之衝擊，陸續檢討該國之個資法相關規定，為與國際接軌，我國亦持續檢討國內個人資料保護法(以下稱個資法)之相關規定，俾使我國個資法對民眾個資之保護程度與先進國家相當；同時，行政院於110年1月啟動之「臺灣開放政府國家行動方案」的「強化數位隱私與個資保護」承諾事項，以及刻正研議之「國家人權行動計畫」子議題，均將個資法特定規範之修正納入檢討，是本研究即需就下列議題比較法規與分析，對我國個資法提出相關具體指引文件或修法條文建議。

一、當事人拒絕權

本議題源於「臺灣開放政府國家行動方案」中的承諾事項1-3「強化數位隱私與個資保護」，欲探究者為「現行個資法就停止蒐集、處理或利用及拒絕行銷部分設有相關規定，該等權利與拒絕權之意涵相似，惟除前開情形外，可否允許個資當事人於一定條件下，拒絕個資保有機關處理或利用其個資」。

對此，本議題即須針對「個資當事人拒絕個資保有機關處理或利用其個資之要件及配套措施（包含但不限於：當事人得否進一步主張銷毀其個資）之可行性」。

二、當事人查詢或請求閱覽權

本議題源於「臺灣開放政府國家行動方案」中的承諾事項1-3「強化數位隱私與個資保護」，欲探究者為「現行個資法雖有規定當事人查詢或請求閱覽權，惟於數位經濟蓬勃發展下，

是否可透過指引等方式，進一步釐清當事人在網路上從事之活動或行為所產生紀錄之查詢範圍等」。

對此，本議題即須針對「個資當事人在網路上從事之活動或行為所產生之紀錄，是否有權向個資蒐集機關查詢或請求閱覽其個資是否正被運用，及查詢或請求閱覽其個資運用之範圍等」進行研議。

三、告知目的外利用或利用開放資料為自動化決策

本議題源於「臺灣開放政府國家行動方案」中的承諾事項1-3「強化數位隱私與個資保護」，基於「現行個資法對直接或間接蒐集個資之告知設有相關規定，惟針對『特定目的外』或『利用開放資料經自動化處理做成決定』等情形，皆未要求告知」，是本議題擬就「目的外利用」及「利用開放資料經自動化處理做成決定」等情形之告知要件及配套措施之可行性，進行研議。

四、個資外洩通知[1]

本議題源於「臺灣開放政府國家行動方案」中的承諾事項1-3「強化數位隱私與個資保護」，欲探究者為「現行個資法雖有規定當個資侵害發生時，應查明後以適當方式通知當事人，惟通知當事人之方式、項目等尚未有明確規定，是否可透過指引等方式說明，以供各界參考」。

對此，本議題即須特別針對「為有效控制損害之擴大，針對包括個資被竊取、洩漏等侵害事件發生時，如何通知當事人及通知當事人之項目」進行研議。

五、當事人同意

[1] 先予敘明者，「臺灣開放政府國家行動方案」以「個資外洩通知」統稱本承諾事項，惟實務上個人資料之安全侵害可能有竊取、竄改、毀損、滅失、洩漏等多種樣態。為防範對應通知事故範圍之誤解，下文討論中，將以「個資侵害事故」稱之。

本議題源於「臺灣開放政府國家行動方案」中的承諾事項1-3「強化數位隱私與個資保護」，由於「現行個資法雖規定『當事人（書面）同意』為蒐集、處理或利用之合法要件之一，惟目前採用之同意方式過於概括或所需同意之內容過於複雜，常發生爭議」，對此，本議題即須針對「個資法同意之意涵、要件明確性及配套措施（包括但不限於：當事人撤回其同意之時機與要件）」進行研議。

六、個資衝擊影響評估[2]

本議題源於「臺灣開放政府國家行動方案」中的承諾事項1-3「強化數位隱私與個資保護」，欲探究者為「現行個資法施行細則雖有規定得採行『個資之風險評估及管理機制』措施，惟哪些業務需進行評估及如何評估，尚不明確，是否可透過指引等方式釐清適用範圍、情形等」。對此，本議題即須針對「個資衝擊影響評估之適用情況、範圍與評估內容要件及配套措施」進行研議。

七、個資保護官（DPO）[3]

本議題源於「國家人權行動計畫」中的「數位人權」議題，由於個資法第 18 條雖要求公務機關指定專人辦理個人資料檔案安全維護事項、個資法施行細則第 12 條第 2 項亦將「配置管理之人員及相當資源」列為公務機關及非公務機關得採行之安全維護措施之一，但前述「專人」或「管理之人員」之職責為何尚不明確，可否兼任其他事務、其職責與執行職務配套措施如何等問題，亦屬未定。對此，本議題即針對「公務機關及非公

[2]「臺灣開放政府國家行動方案」本承諾事項所稱之「個資衝擊影響評估」應係源於英文 Data Protection Impact Assessment (DPIA)，於我國實務上又稱「個資保護影響評估」。

[3]「國家人權行動計畫」中「數位人權」議題一節稱之「個資保護官」，應係源於GDPR所規範之 Data Protection Officer (DPO)，於我國實務上又稱「個資保護長」。

務機關設置個資保護官之必要性、設置條件及相關配套措施」進行研議。

第二章　研究方法

本研究將以法規比較法為原則，針對指定議題就研究國家的個人資料保護或隱私法律詳為分析，比較研究國家法律與我國個人資料保護法之差異，就我國法律可借鏡之處提出建議。此外，本研究亦將以文獻分析法，整理研究國家個人資料或隱私保護法規主管機關就指定議題曾發布之實務指引，以及學者專家就指定議題發表的相關文獻，以此作為本研究提出修法條文草案或指引草案內容之參考。比較國家法律包含：

一、歐盟個人資料保護規則（General Data Protection Regulation）

歐盟於 2016 年通過個人資料保護規則（General Data Protection Regulation, GDPR），並於 2018 年 5 月正式施行。

較之於此前的 1995 年個人資料保護指令（Data Protection Directive）[4]，GDPR 在歐洲經濟區建立起通用之個資保護法律制度，賦予個資當事人更豐富、更有力的資料權利，強化個資控管者（controller）之透明化（transparency）與問責要求，引入個資侵害事故通知、個資衝擊影響評估（Data Protection Impact Assessment, DPIA）、個資保護官（Data Protection Officer, DPO）等資料保護之諸多新制度，並發展出一套新的資料治理體系[5]。

二、美國加州消費者隱私法（California Consumer Privacy Act）

美國加州於於 2018 年通過加州消費者隱私保護法（California Consumer Privacy Act, CCPA），並於 2020 年 1 月正

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[5] European Commission, Data Protection as A Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation (COM(2020) 264 final, 24 June 2020).

式施行，是美國首部全面規範消費者隱私保護的州級法律，構建出可與歐盟 GDPR 類比之消費者個資權利保護框架。

2020 年 11 月美國大選期間，加州人民公投通過加州隱私權法（California Privacy Rights Act, CPRA），對 CCPA 作出大規模增修，其中包含強化當事人知情同意規範、新增個資衝擊影響評估要求等。

三、美國維吉尼亞州消費者資料保護法（Virginia Consumer Data Protection Act）

美國維吉尼亞州於 2021 年 3 月通過消費者資料保護法（Consumer Data Protection Act, CDPA），並將於 2023 年 1 月 1 日施行。

該法採類似 GDPR 之個資保護框架，賦予消費者近用權、拒絕權等共 6 項資料保護權利，以「控管者」為資料保護之首要責任者，且將透明化作為控管者主要責任之一。該法亦強制要求高風險處理前執行個資衝擊影響評估。

四、日本個人資訊保護法（個人情報の保護に関する法律）

日本的個人資料保護法律有其獨特立法架構。公部門與民間部門皆須遵守之個資保護基本原則，定於個人資訊保護法（個人情報の保護に関する法律）第一章至第三章，但該法之其餘章節，僅規範民間部門之個資保護責任。行政機關及獨立行政法人之個資保護責任，則分別以其他法律規範[6]。日本現行個人資訊保護法於 2003 年頒行，於 2020 年（令和二年）6 月 12 日作實質修正，將於 2022 年（令和四年）4 月 1 日全面施行。此次修正對當事人拒絕權、個資侵害事故通知等作出較大變革。

[6] 行政機関の保有する個人情報の保護に関する法律（平成十五年法律第五十八号）；独立行政法人等の保有する個人情報の保護に関する法律（平成十五年法律第五十九号）。

日本國會又於 2021 年 5 月通過「數位社會構建規畫相關法律整備法」（以下稱數位社會整備法）[7]。該法將打破日本現行民間部門、行政機關、獨立行政法人三部個資法並行之局面，將公部門主體亦納入個人資訊保護法之適用範圍，使個人資訊保護法成為普遍適用於各類主體之個人資訊保護法律。數位社會整備法之施行日期，將由政令另行確定。

本報告將以定於 2022 年 4 月 1 日全面施行之個人資訊保護法為主要研究對象。如數位社會整備法對相關規範有實質修改，本報告將於各相關章節一併敘明。

五、韓國個人資料保護法（개인정보 보호법）

韓國之資料保護以「數據 3 法」，即個人資料保護法（개인정보보호법）、資訊通信網法（정보통신망법）和信用資料法（신용정보법）三部法律為核心。

韓國國會於 2020 年 1 月通過、同年 8 月施行數據 3 法修正案，大幅修正個人資料保護法內容，刪除另外兩部法律中重複性條文，形成個人資料保護法包含普適性規範，資訊通信網法和信用資料法包含特殊個資保護規範之架構[8]。

六、新加坡個人資料保護法（Personal Data Protection Act）

新加坡現行個人資料保護法（Personal Data Protection Act, PDPA）於 2012 年制定。2020 年 11 月，新加坡國會通過該法最近一次修正，大幅修正無需當事人同意即可蒐集、利用或揭露

[7] デジタル社会の形成を図るための関係法律の整備に関する法律（令和三年法律第三十七号）。

[8] 韓國 2020 年最新修正之個人資料保護法中韓對照全文，請參本事務所曾受國家發展委員會委託研究「韓國個人資料保護法制因應 GDPR 施行之調適」研究案結案報告：https://www.ndc.gov.tw/News_Content.aspx?n=B7C121049B631A78&sms=FB990C08B596EA8A&s=11BA2EA8D67710C9。又韓國政府出資設置之韓國法律研究所（한국법제연구원）亦提供韓國個人資料保護法及其施行細則之英文全文翻譯，詳見：https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG；https://elaw.klri.re.kr/eng_service/lawView.do?hseq=54521&lang=ENG。

資料之規範，並引入強制性個資侵害事故通知與個資衝擊影響評估制度。該修正已於 2021 年 2 月生效。

第三章　研究議題

第一節 當事人拒絕權

一、議題釐清

本議題源於「臺灣開放政府國家行動方案」中的承諾事項 1-3「強化數位隱私與個資保護」[9]，欲探究者為「現行個資法就停止蒐集、處理或利用及拒絕行銷部分設有相關規定，該等權利與拒絕權之意涵相似，惟除前開情形外，可否允許個資當事人於一定條件下，拒絕個資保有機關處理或利用其個資」。對此，本議題即須針對「個資當事人拒絕個資保有機關處理或利用其個資之要件及配套措施（包含但不限於：當事人得否進一步主張銷毀其個資）之可行性」，特別是「即便蒐集機關合法處理或利用個人資料時，當事人有無權利拒絕其處理或利用個資之行為」進行研議。

需先敘明，各國個人資料保護法律多有以「當事人同意」作為蒐集、處理與利用個人資料之合法要件者，無論該法是否明文規定當事人「撤回」其同意之權利，在蒐集機關基於當事人同意而持續蒐集、處理或利用個人資料的情形，當事人既可依其自由意願對蒐集機關之行為表示同意（當事人資訊自主權的落實），自可依其自由意願撤回該同意。此時，倘蒐集機關別無其他合法要件蒐集、處理與利用個人資料，即應停止該行為，則當事人撤回同意的效果即等同於當事人拒絕蒐集機關原本合法的行為，與本議題討論的拒絕權的行使相似。因此以下於比較法規時，遇有當事人同意撤回之情形即暫不於本節拒絕權討論。

二、我國個人資料保護法

個人資料保護法（下稱個資法）第 3 條第 4 款規定「當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：...四、請求停止蒐集、處理或利用」。是在我國個資法規範下，

[9] 臺灣開放政府國家行動方案，2021 年 4 月，頁 12-15。

當事人尚非可任意請求蒐集機關停止處理或利用其個人資料，須視是否符合個資法規定的相關要件。

（一）正確性爭議

個資法第 11 條第 2 項規定「個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議者，不在此限」。此處當事人請求停止處理或利用個人資料，與蒐集機關之行為是否違法無關，係因對其個人資料之正確性存有爭議，在蒐集機關更正或雙方釐清爭議前，為免不正確之資料造成不正確的結果，因此允許當事人可要求蒐集機關「暫停」處理或利用該個人資料之行為。

（二）特定目的消失

個資法第 11 條第 3 項規定「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限」。

由於蒐集、處理與利用個人資料除須符合個資法允許的合法要件之外，尚以「有特定目的」為前提，是當特定目的消失時，其合法要件即已不存在，當事人就此要求停止處理或利用，進而要求刪除個人資料，此為法理之必然。

（三）違法行為

個資法第 11 條第 4 項規定「違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料」。

由於蒐集機關的違法行為本即不應允許，是本項規定賦予當事人得要求蒐集機關停止為該違法行為之權利，乃屬當然。

（四）合法行銷

個資法第 20 條第 2 項規定「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」，此即謂縱使非公務機關合法對當事人利用其個人資料行銷，當事人仍有權隨時拒絕接受該行銷行為。

（五）一般來源資料

個資法第 19 條第 1 項第 7 款規定「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，顯有更值得保護之重大利益者，不在此限」。

此處所稱「一般可得之來源」，依個資法施行細則第 28 條規定係指「透過大眾傳播、網際網路、新聞、雜誌、政府公報及其他一般人可得知悉或接觸而取得個人資料之管道」。其立法理由乃考量資訊科技及網際網路之發達，涉及個人資料之行為甚為普遍，尤其在網際網路上張貼之個人資料其來源是否合法，經常無法求證或需費過鉅，為避免蒐集者動輒觸法或求證費時，將本款列為非公務機關得合法蒐集、處理與利用一般個人資料之合法要件，並為兼顧當事人重大利益而定有但書。

又依個資法第 19 條第 2 項之規定，若蒐集或處理者知悉或經當事人通知前述「禁止處理或利用個人資料」之意時，即應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

因此，即便蒐集機關以「個人資料取自於一般可得之來源」而合法蒐集、處理與利用個人資料，惟當事人「禁止處理或利用個人資料」之通知，將使蒐集機關不得再繼續處理或利用其個人資料，其效果等同拒絕權之行使。

綜合上述規定，我國個資法對於蒐集機關的合法行為，僅於「非公務機關蒐集、處理與利用取自於一般可得之來源的個人資料」，以及「非公務機關利用個人資料行銷」之情形，賦予當事人拒絕之權。

至於拒絕後得否請求刪除個人資料，則回歸個資法第 11 條第 3 項或第 4 項規定判斷。

三、外國立法例

（一）歐盟 GDPR

歐盟 GDPR 於第三章規範當事人權利，其中與本議題相關者為第 17 條的刪除權（Right to Erasure）、第 18 條的限制處理權（Right to Restriction of Processing）、第 21 條的拒絕權（Right to Object）及第 22 條的拒絕自動化決策權。

須留意的是，依 GDPR 第 23 條之意[10]，歐盟或會員國法律得在尊重基本權與自由的本質，且屬於民主社會中保障、維護特定目的（例如國家或公共安全、犯罪偵查、重要公益、

[10] EU, GDPR, §23(1), "Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: (a) national security; (b)defence; (c) public security; (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security; (f) the protection of judicial independence and judicial proceedings; (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g); (i) the protection of the data subject or the rights and freedoms of others; (j) the enforcement of civil law claims."

保護當事人、保護他人的權利與自由等）所必要且合於比例原則之措施時，立法限制上述權利。

1、拒絕基於公益或正當利益之處理、拒絕行銷與拒絕後刪除權

GDPR 第 21 條第 1 項規定[11]，當事人依其個案情形，有權隨時拒絕基於公共利益（包含執行公務或受託行使公權力）或正當利益處理其個人資料，包含對當事人為剖析（profiling）行為。控管者應即停止處理該個人資料，但控管者能證明其處理行為具有優於當事人的利益、權利或自由之正當理由，或證明處理行為是為建立、行使或防禦法律請求所需者，不在此限。

GDPR 前言第 69 點指出[12]，雖然個人資料可能基於公共利益之任務執行或受託行使公權力，或基於控管者或第三人的正當利益而被合法的處理，但當事人仍有權根據個案情形拒絕處理任何個人資料。

在當事人依上述規定行使拒絕權而尚待控管者確認其正當利益是否優於當事人的正當利益時，依 GDPR 第 18 條第 1 項第 d 款規定[13]，當事人有權限制控管者處理個人資料。此時，系爭個人資料除為儲存之目的外，僅在「基於當事人同意」或「為建立、行使或防禦法律上請求」或「為保障其他自然

[11] EU, GDPR, §21(1), "The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims."

[12] EU, GDPR, Recital §69, "Where personal data might lawfully be processed because 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 controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation……"

[13] EU, GDPR, §18(1)(d), "The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:…(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject."

人或法人之權利」或「基於歐盟或會員國的重要公共利益之理由」的情形下始得繼續處理(GDPR 第 18 條第 2 項規定)[14]。

GDPR 前言（Recital）第 67 點並指出[15]，限制處理個人資料的方式包含但不限於「暫時將經選取的資料移至其他處理系統」、「讓使用者無法取得經選取的資料」或「自網站上暫時移除曾公開的資料」。

另當個人資料被用於行銷（direct marketing）的目的時，依 GDPR 第 21 條第 2 項規定[16]，當事人有權隨時拒絕為該行銷而處理其個人資料，包含在行銷範圍內的剖析行為。同條第 3 項並規定[17]，一經當事人表示拒絕為行銷目的處理個人資料，該個人資料即不得再為該目的而被處理。

而在當事人依 GDPR 第 21 條第 1 項拒絕處理個資行為，且該處理行為不存在優勢正當理由，或當事人依 GDPR 第 21 條第 2 項拒絕行銷行為時，依 GDPR 第 17 條第 1 項第 c 款規定[18]，當事人有權請求控管者即時刪除其個人資料，控管者有義務即時刪除。

2、拒絕研究

如個人資料基於科學或歷史研究，或統計目的而被處理時（在符合 GDPR 第 89 條第 1 項規定之安全維護措施要件的

[14] EU, GDPR, §18(2), "Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State."

[15] EU, GDPR, Recital §67, "Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website."

[16] EU, GDPR, §21(2), "Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing."

[17] EU, GDPR, §21(3), "Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes."

[18] EU, GDPR, §17(1)(c), "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:…(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2)…"

前提下），GDPR 第 21 條第 6 項規定[19]，當事人依其個案情形，有權拒絕處理其個人資料，但該處理行為是為公共利益之任務執行所必須者，不在此限。

至於當事人拒絕此行為後，仍應視是否符合 GDPR 第 17 條規定以判斷當事人刪除權的行使條件。

GDPR 第 17 條第 1 項規定[20]，當滿足下列條件之一時，當事人有權請求控管者即時刪除其個人資料，控管者有義務即時刪除：(1)該個人資料對於蒐集或處理的目的已非必要時；(2)當處理該個人資料的合法要件為 GDPR 第 6 條第 1 項第 a 款或第 9 條第 2 項第 a 款的「當事人同意」，而當事人撤回其同意，且不存在其他處理個人資料的合法要件時；(3)當事人依 GDPR 第 21 條第 1 項拒絕處理個資行為，且該處理行為不存在優勢正當理由，或當事人依 GDPR 第 21 條第 2 項拒絕行銷行為時；(4)該個人資料遭違法處理時；(5)當控管者受歐盟或會員國法律拘束，須將該個人資料刪除以遵守法律義務時；(6)該個人資料係依 GDPR 第 8 條第 1 項規定，為提供資訊社會服務所蒐集時。

然而，依同條第 3 項規定[21]，當處理個資行為是為下列情形之一所必要時，前述當事人刪除權（或控管者的刪除義務）

[19] EU, GDPR, §21(6), "Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest."

[20] EU, GDPR, §17(1), "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e)the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)."

[21] EU, GDPR, §17(3), "Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:(a) for exercising the right of freedom of expression and information; (b)for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject

規定即不適用：(1)為行使言論自由或資訊權；(2)控管者依所適用的歐盟或會員國法律，為遵守法律義務而須處理個人資料，或基於公共利益而執行任務，或受託行使公權力；(3)依 GDPR 第 9 條第 2 項第 h 款與第 i 款，以及第 9 條第 3 項，為公共衛生領域的公共利益理由處理個人資料；(4)依 GDPR 第 89 條第 1 項規定，為符合公共利益之建檔目的、科學或歷史研究目的或統計目的，且當事人行使刪除權將有可能導致處理個人資料行為之目的不可能達成，或嚴重阻礙其達成時；(5)為建立、行使或防禦法律上請求。

因此，如控管者為公共利益之任務執行，基於科學或歷史研究，或統計目的，在符合 GDPR 第 89 條第 1 項規定之安全維護措施要件的前提下處理個人資料時，當事人之拒絕權本即受到限制（GDPR 第 21 條第 6 項但書），亦無所謂拒絕後的刪除權。至若控管者非因公共利益之任務執行而為研究目的處理個人資料時，當事人對此合法行為可隨時表示拒絕，並依 GDPR 第 17 條第 1 項及第 3 項的原則與例外要件，檢視可否行使刪除權。

3、拒絕自動化決策

GDPR 第 22 條規定，當事人有權不受「完全根據自動化處理（包含剖析）而對其產生法律效果或類似重大效果之決定」的拘束[22]，除非該決定(1)是為締結或履行當事人與控管者之間的契約所必要；或(2)是控管者依其適用之歐盟法或會

or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c)for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); (d)for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e)for the establishment, exercise or defence of legal claims."

[22] EU, GDPR, §22(1), "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

員國法所允許，且該法律亦規範保障當事人權利、自由與正當利益的適當措施；或(3)是基於當事人明確表示之同意[23]。

但在前述「締約、履約」或「當事人同意」的情形，控管者應採取保障當事人權利、自由與正當利益的適當措施，至少讓當事人有權獲得控管者人為介入的機會，表達其論點，並對該決定提出質疑[24]。

雖然條文並未使用「拒絕（object）」一詞，但由文義理解可知，應指當事人有權拒絕控管者完全根據自動化決策即對其作出產生法律效果或類似重大效果之決定。至於當事人拒絕後的刪除權行使，則仍應依 GDPR 第 17 條規定檢視。

由上述規定可知，歐盟 GDPR 允許當事人對控管者依特定合法要件（為執行公務或受託行使公權力之公共利益，或為正當利益）處理個人資料之行為行使拒絕權；亦允許當事人對控管者基於特定目的之行為行使拒絕權（行銷、研究、自動化決策），皆為對「合法」行為之拒絕權（但有例外）。

（二）美國加州 CCPA

加州消費者隱私法（California Consumer Privacy Act, CCPA）第 1798.120 條規定，消費者有權隨時向出售或分享其個人資料之業者，要求不得再出售或分享其個人資料予第三人（拒絕出售或分享權，Right to Opt-Out of Sale or Sharing）。

[23] EU, GDPR, §22(2), "Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent."

[24] EU, GDPR, §22(3), "In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."

而業者有義務依法定要件向消費者告知其個人資料將被出售或分享予第三人，並告知消費者有權隨時行使前述拒絕權[25]。

另如業者明知消費者未滿16歲時，除非該消費者已滿13歲而明確授權（has affirmatively authorized），或該消費者未滿 13 歲而由其父母或監護人明確授權，否則業者亦不得出售或分享該消費者個人資料。且倘業者刻意忽略消費者年齡時，依法即視為明知該消費者的年齡[26]。

當業者接獲前揭拒絕權的行使要求，或在消費者未成年而未獲得前述合法同意時，即不得出售或分享該消費者的個人資料，除非事後獲得該消費者的同意[27]。惟依 CCPA 第1798.135條第c項第4款規定，業者在消費者行使拒絕權後，須待至少 12 個月始得再次徵求消費者同意出售或分享其個人資料[28]。

[25] California, CCPA (as amended by CPRA), §1798.120(a), " A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. This right may be referred to as the right to opt-out of sale or sharing". §1798.120(b), "A business that sells consumers' personal information to, or shares it with, third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold or shared and that consumers have the "right to opt-out" of the sale or sharing of their personal information."

[26] California, CCPA (as amended by CPRA), §1798.120(c), "Notwithstanding subdivision (a), a business shall not sell or share the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale or sharing of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age."

[27] California, CCPA (as amended by CPRA), §1798.120(d), "A business that has received direction from a consumer not to sell or share the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell or share the minor consumer's personal information, shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from selling or sharing the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides consent, for the sale or sharing of the consumer's personal information."

[28] California, CCPA (as amended by CPRA), §1798.135(c)(4), "For consumers who exercise their right to opt-out of the sale or sharing of their personal information or limit the use or disclosure of their sensitive personal information, refrain from selling or sharing the consumer's personal information or using or disclosing the consumer's sensitive personal information and wait for at least 12 months before requesting that the consumer authorize the sale or sharing of the consumer's personal information or the use and disclosure of the consumer's sensitive personal information for additional purposes, or as authorized by regulations."

此外，CCPA 第 1798.115 條第 d 項規定，向業者購得或獲提供分享消費者個人資料之第三人，在消費者接獲明確通知並有機會向該第三人行使拒絕權之前，不得將該消費者個人資料再為出售或分享[29]。

另因 CCPA 第 1798.105 條第 a 項賦予消費者原則皆得請求業者刪除自消費者取得之個人資料的權利。但業者如符合同條第 d 項之例外事由，例如個資資料係完成與該消費者間交易所必要、保障業者或第三人之言論自由、行使法定權利、履行法定義務、僅供業者內部利用（但以符合消費者合理期待為限）等，則無需遵守消費者之刪除請求[30]。是無論消費者是否依前述規定行使拒絕權，均可行使 CCPA 中的刪除權。

由上述規定可知，CCPA 一方面賦予消費者任意請求業者刪除個人資料之權（效果同於任意拒絕業者為任何目的處理其個人資料），二方面又賦予消費者可拒絕業者依特定目的（出售或分享其個人資料）處理其個人資料之權利。由於 CCPA 並未規範「合法」蒐集、處理或利用個人資料的合法要件（前提要件），因此 CCPA 中的拒絕權即可視為係以業者的合法行為為拒絕標的。

另依 CCPA 第 1798.185 條第 a 項第 16 款，州檢察長應制定施行細則，規定業者使用自動化決策技術（包括剖析）處理個人資料時，消費者之近用權和拒絕權，並要求業者在回應消費者請求時，提供關於決策邏輯有意義之資訊，以及處理對消費者可能造成的後果。此一規範自 2020 年 12 月生效，但截至 2021 年 11 月，加州州檢察長尚未公布相關施行細則。2020 年 CPRA 修正 CCPA，設立加州隱私保護署（California

[29] California, CCPA (as amended by CPRA), §1798.115(d), "A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120."

[30] California, CCPA (as amended by CPRA), §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."

Privacy Protection Agency）。待加州隱私保護署啟動運作後，制定施行細則之權力將移交該署行使[31]。2021 年 9 月，加州隱私保護署發布公告（以下稱「CPRA 細則公告」），就訂定施行細則事宜初步徵求民眾意見，其中包含「自動化決策」及「剖析」之含義、近用權與拒絕權行使之範圍與程序、業者回應消費者請求之實質要求等[32]。因此，CCPA 關於自動化決策（剖析）之施行細則，將待加州隱私保護署制定。

（三）美國維吉尼亞州 CDPA

維吉尼亞州消費者資料保護法（Consumer Data Protection Act, CDPA）第 59.1-573 條第 A 項規定[33]，消費者（或其父母或法定監護人）得隨時向控管者提出申請，就其個人資料行使消費者權利。同項第 5 款即賦予消費者對於控管者將其個人資料用於：(1)精準廣告；(2)出售個人資料；(3)為作成對該消費者發生法律效力或類似重大效果之決定所為的剖析（profiling）等 3 種目的之拒絕權[34]。此外，同項第 3 款亦賦予消費者對自己提供或由控管者另行取得之個人資料，得向控管者行使之刪除權[35]。

然而，對於前述拒絕權與刪除權（以及 CDPA 中的其他消費者權利），CDPA 於第 59.1-578 條第 B 項訂有例外規定[36]，

[31] California, CCPA (as amended by CPRA), §1798.185(d).

[32] California Privacy Protection Agency, Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 (September 22, 2021), https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf.

[33] Virginia, CDPA, §59.1-573(A), "A consumer may invoke the consumer rights authorized pursuant to this subsection at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to invoke. A known child's parent or legal guardian may invoke such consumer rights on behalf of the child regarding processing personal data belonging to the known child. A controller shall comply with an authenticated consumer request to exercise the right:…"

[34] Virginia, CDPA, §59.1-573(A)(5), "To opt out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer."

[35] Virginia, CDPA, §59.1-573(A)(3), "To delete personal data provided by or obtained about the consumer."

[36] Virginia, CDPA, §59.1-578(B), "The obligations imposed on controllers or processors under this chapter shall not restrict a controller's or processor's ability to collect, use, or retain data to: 1. Conduct internal research to develop, improve, or repair products, services, or technology; 2. Effectuate a

CDPA 所規範之控管者（或受託處理者）各項義務，不限制控管者（或受託處理者）為下列目的蒐集、利用或保存資料之權益：

1、為開發、改良或維修產品、服務或技術而執行內部研究；

2、發起產品召回；

3、識別並修復對性能造成損害之既存或預期中的技術瑕疵；

4、執行「與消費者之期待具有合理一致性」或「根據消費者與控管者的現有關係可合理預期」或「其他適於『為促進消費者特別要求的產品或服務之提供』或『為促進履行與消費者間之契約』而處理個人資料」的內部行為。

而若控管者適用前述第 59.1-578 條第 B 項（或該條其他項）的義務豁免例外事由時，同條第 G 項規定[37]，應由控管者就該事由負舉證之責。

不過，雖然第 59.1-578 條第 B 項對控管者的義務定有例外，但對照第 59.1-573 條第 A 項第 5 款列出消費者得拒絕控管者利用個人資料的事由（精準廣告、出售個人資料、為作成對該消費者發生法律效力或類似重大效果之決定所為的剖析）來看，由於第59.1-578條第B項所列例外事由或限於「內部利用」，或具有保護消費者權益之目的，當消費者針對此三種目的行使拒絕權時，由實務運作角度觀之，控管者似乎難援用第 59.1-578 條第 B 項的例外事由與之對抗。

由上述規定可知，CDPA 與 CCPA 相似，一方面賦予消費者任意請求控管者刪除個人資料之權（效果同於任意拒絕

product recall; 3. Identify and repair technical errors that impair existing or intended functionality; or 4. Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party."

[37] Virginia, CDPA, §59.1-578(G), "If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in subsection F."

控管者為任何目的處理其個人資料），二方面又賦予消費者可對特定目的（精準廣告、出售個人資料、為作成對該消費者發生法律效力或類似重大效果之決定所為的剖析）拒絕控管者處理其個人資料之權利。但 CDPA 亦給予控管者援用例外事由、豁免滿足消費者行使前述權利之機會，惟須由控管者就符合例外事由之事實承擔舉證責任（且如前述，控管者實際上似較難主張例外事由，對抗消費者就前揭特定目的行使之拒絕權）。又 CDPA 亦未規範「合法」蒐集、處理或利用個人資料的合法要件（前提要件），因此 CDPA 中的拒絕權亦可視為係以控管者的合法行為為拒絕標的。

（四）日本個人資訊保護法

其中第 30 條第 1 項規定[38]，若個人資訊處理事業違法取得或利用可識別當事人之個人資料時，當事人有權要求停止利用或刪除其個人資料。同條第 2 項規定[39]，當個人資訊處理事業接獲當事人請求並認為有理由時，應即時停止利用或刪除個人資料，以改正違法情形。但停止利用或刪除個人資料將耗費過鉅或有困難，且個人資訊處理事業採取必要的替代措施以確保當事人權益者，不在此限。

又第 30 條第 3 項規定[40]，如個人資訊處理事業違法將可識別當事人之個人資料提供給第三人時，當事人有權要求個

[38] 日本，個人情報保護法，§30(1)，「本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データが第 16 条の規定に違反して取り扱われているとき又は第 17 条の規定に違反して取得されたものであるときは、当該保有個人データの利用の停止又は消去（以下この条において「利用停止等」という。）を請求することができる」。

[39] 日本，個人情報保護法，§30(2)，「個人情報取扱事業者は、前項の規定による請求を受けた場合であって、その請求に理由があることが判明したときは、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行わなければならない。ただし、当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない」。

[40] 日本，個人情報保護法，§30(3)，「本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データが第 23 条第 1 項又は第 24 条の規定に違反して第三者に提供されているときは、当該保有個人データの第三者への提供の停止を請求することができる」。

人資訊處理事業停止提供。同條第 4 項規定[41]，當個人資訊處理事業接獲當事人請求並認為有理由時，應即時停止向第三人提供當事人之個人資料。但停止提供個人資料予第三人將耗費過鉅或有困難，且個人資訊處理事業採取必要的替代措施以確保當事人權益者，不在此限。

另第 30 條第 5 項規定[42]，當「個人資訊處理事業已無必要利用可識別當事人之個人資料」，或「個人資料有洩漏、遺失、損害或其他與個人資料安全維護有關之情形，且該情形經個資保護委員會規定為對當事人權益有造成侵害的高度可能」，或「處理可識別當事人的個人資料將可能侵害當事人的權利或正當利益」時，當事人得要求個人資訊處理事業停止利用或刪除其個人資料，或停止將個人資料提供給第三人。同條第 6 項規定[43]，當個人資訊處理事業接獲當事人請求並認為有理由時，應即時停止利用或刪除該個人資料，或停止向第三人提供個人資料，以在必要範圍內避免當事人權益受侵害。但停止利用或刪除個人資料，或停止提供個人資料予第三人將耗費過鉅或有困難，且個人資訊處理事業採取必要的替代措施以確保當事人權益者，不在此限。

---

[41] 日本，個人情報保護法，§30(4)，「個人情報取扱事業者は、前項の規定による請求を受けた場合であって、その請求に理由があることが判明したときは、遅滞なく、当該保有個人データの第三者への提供を停止しなければならない。ただし、当該保有個人データの第三者への提供の停止に多額の費用を要する場合その他の第三者への提供を停止することが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない」。

[42] 日本，個人情報保護法，§30(5)，「本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データを当該個人情報取扱事業者が利用する必要がなくなった場合、当該本人が識別される保有個人データに係る第二十二条の二第一項本文に規定する事態が生じた場合その他当該本人が識別される保有個人データの取扱いにより当該本人の権利又は正当な利益が害されるおそれがある場合には、当該保有個人データの利用停止等又は第三者への提供の停止を請求することができる。」。

[43] 日本，個人情報保護法，§30(6)，「個人情報取扱事業者は、前項の規定による請求を受けた場合であって、その請求に理由があることが判明したときは、本人の権利利益の侵害を防止するために必要な限度で、遅滞なく、当該保有個人データの利用停止等又は第三者への提供の停止を行わなければならない。ただし、当該保有個人データの利用停止等又は第三者への提供の停止に多額の費用を要する場合その他の利用停止等又は第三者への提供の停止を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない」。

最後，第 30 條第 7 項規定[44]，個人資訊處理事業對當事人停止利用或刪除個人資料，或停止提供個人資料予第三人之請求，無論針對全部或部分個人資料接受或拒絕當事人之請求，皆應即時將該決定通知當事人。且依第 31 條規定[45]，此通知內容應包含向當事人解釋個人資訊處理事業拒絕當事人全部或部分要求，或將採取與當事人之要求相異的替代措施之理由。

由上述法規可知，日本個人資訊保護法賦予當事人的停止利用（與刪除）權，以符合特定條件為前提，其一係個人資訊處理事業「違法」取得或利用（包含將個人資料提供予第三人）個人資料；其二為「個人資訊處理事業已無必要利用可識別當事人之個人資料」；其三為「個人資料有洩漏、遺失、損害或其他與個人資料安全維護有關之情形，且該情形經個資保護委員會規定為對當事人權益有造成侵害的高度可能」；其四則是「處理個人資料將可能侵害當事人的權利或正當利益」。於該法配合數位社會整備法修正後，前開規範雖有條號及文字調整，但其內容並無實質變化。

（五）日本行政機關個人資訊保護法

日本行政機關個人資訊保護法第 36 條第 1 項規定[46]，任何人如認為自己的個人資料有下列各款情形之一時，得依本

[44] 日本，個人情報保護法，§30(7)，「個人情報取扱事業者は、第一項若しくは第五項の規定による請求に係る保有個人データの全部若しくは一部について利用停止等を行ったとき若しくは利用停止等を行わない旨の決定をしたとき、又は第三項若しくは第五項の規定による請求に係る保有個人データの全部若しくは一部について第三者への提供を停止したとき若しくは第三者への提供を停止しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない」。

[45] 日本，個人情報保護法，§31，「個人情報取扱事業者は、第二十七条第三項、第二十八条第三項（同条第五項において準用する場合を含む。）、第二十九条第三項又は前条第七項の規定により、本人から求められ、又は請求された措置の全部又は一部について、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合には、本人に対し、その理由を説明するよう努めなければならない」。

[46] 日本，行政機關個人情報保護法，§36(1)，「何人も、自己を本人とする保有個人情報が次の各号のいずれかに該当すると思料するときは、この法律の定めるところにより、当該保有個人情報を保有する行政機関の長に対し、当該各号に定める措置を請求することができ

法規定，向保有該個人資料之行政機關首長請求各款所定之處置。但當該個人資料的停止利用、刪除或停止提供，依其他法律或依法發布之命令而有特別程序者，不在此限：(1)該行政機關違法取得個人資料，或違反第3條第2項規定（逾越達成法定職務目的之必要範圍）而保存個人資料，或違反第8條第1項及第2項規定，即未符合例外事由，於目的外利用個人資料時，可請求停止利用或刪除個人資料；(2)違反第 8 條第1項及第2項規定提供個人資料時，可請求停止提供。

由此可知，日本行政機關個人資訊保護法未賦予當事人拒絕行政機關合法利用個人資料的權利，僅在行政機關違法取得、保存或利用、提供時，當事人始有權拒絕。該法經配合數位社會整備法修正，併入個人資訊保護法後，前開規範雖有條號及文字調整，但其內容並無實質變化。

（六）韓國個人資料保護法

韓國個人資料保護法第 15 條第 1 項規定[47]，個人資料處理者在符合下列合法要件之一時，始得蒐集個人資料，並於蒐集目的範圍內利用：

る。ただし、当該保有個人情報の利用の停止、消去又は提供の停止（以下「利用停止」という。）に関して他の法律又はこれに基づく命令の規定により特別の手続が定められているときは、この限りでない。一　当該保有個人情報を保有する行政機関により適法に取得されたものでないとき、第三条第二項の規定に違反して保有されているとき、又は第八条第一項及び第二項の規定に違反して利用されているとき　当該保有個人情報の利用の停止又は消去 二　第八条第一項及び第二項の規定に違反して提供されているとき　当該保有個人情報の提供の停止」。

[47] 한국，개인정보보호법，§15(1), “개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다. 1. 정보주체의 동의를 받은 경우 2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우 4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우 5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제 3 자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한

1、取得當事人同意時。

2、法律有特別規定或為遵守法令上義務而不可避免時。

3、公務機關為執行法定職務而不可避免時。

4、為與當事人締約或履行該契約而不可避免時。

5、當事人及其法定代理人陷於無法為意識表示之狀態，或住所不明等而無法取得事前同意，確實有明顯保護當事人及第三方急迫生命、身體、財產利益之必要時。

6、個人資料處理者之正當利益所必要，且該正當利益明顯優先於當事人的權利時。此僅限於與個人資料處理者之正當利益顯著相關且不超過合理範圍之情形。

而韓國個人資料保護法於第 37 條規定當事人之停止處理權，依第 37 條第 1 項規定[48]，當事人對其個人資料之處理行為，有權請求停止。在此情形，如個人資料處理者為公務機關，當事人僅得針對公務機關依照該法第 32 條登錄於個人資料檔案中的個人資料提出停止處理的請求。

경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다."

[48] 한국，개인정보보호법，§37(1), "정보주체는 개인정보처리자에 대하여 자신의 개인정보처리의 정지를 요구할 수 있다. 이 경우 공공기관에 대하여는 제 32 조에 따라 등록 대상이 되는 개인정보파일 중 자신의 개인정보에 대한 처리의 정지를 요구할 수 있다"

同條第 2 項規定[49]，個人資料處理者原則上應即依照當事人的請求，停止處理其個人資料的全部或一部，只在符合下列情形之一時，始得拒絕當事人的權利行使[50]，包含：

1、法律有特別規定或為遵守法令上之義務而不可避免時。

2、有危害他人之生命、身體之虞，或可能侵害他人財產與其他利益之虞時。

3、公務機關如未處理個人資料將無法執行其他法律所定之職務。

4、若未處理個人資料將無法提供當事人約定之服務等致履行契約有困難，而當事人未明確表明解除契約意思時。

又當個人資料處理者依當事人請求而停止處理個人資料時，依第 37 條第 4 項規定[51]，個人資料處理者即應立即採取例如銷毀個人資料等必要措施，不得遲延。

由上述規定可知，韓國個人資料保護法賦予當事人的停止處理權，以「當事人得任意行使」為原則（對於合法蒐集、利用個人資料之行為亦可行使），惟當符合特定情形時，個人資料處理者仍可例外拒絕當事人的行使停止處理權。而比

---

[49] 한국，개인정보보호법，§37(2),"개인정보처리자는 제 1 항에 따른 요구를 받았을 때에는 지체 없이 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다. 1、법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우. 2、다른 사람의 생명・신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우. 3、공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우. 4、개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우"

[50] 此時個人資料處理者應立即將拒絕事由告知當事人，不得遲延。見한국，개인정보보호법，§37(3),"개인정보처리자는 제 2 항 단서에 따라 처리정지 요구를 거절하였을 때에는 정보주체에게 지체 없이 그 사유를 알려야 한다"

[51] 한국，개인정보보호법，§37(4), "개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다"

較第 15 條第 1 項所列合法蒐集、利用個人資料之合法要件與第 37 條第 2 項所列得拒絕當事人行使停止處理權之事由可知，個人資料處理者若基於正當利益蒐集、利用個人資料，而當事人行使停止處理權時，個人資料處理者並無例外事由可拒絕當事人的權利行使。

至於如個人資料處理者無例外事由可適用而須滿足當事人的停止處理權時，韓國個人資料保護法並要求個人資料處理者應在停止處理個人資料後，一併依個案情形採取銷毀（刪除）個人資料等必要措施。

又韓國現行個人資料保護法並未規定個資當事人拒絕自動化決策之權利，亦未就自動化決策之告知或近用權作出特別規範。然韓國個人資料保護委員會於 2021 年 1 月公告個人資料保護法修正案草案並公開徵求意見[52]。該修正案草案計劃新增個資當事人拒絕自動化決策之權利。2021 年 9 月，韓國個人資料保護委員會再度公告個人資料保護法修正草案[53]，擬於該法第 4 條新增第 6 項，明文賦予個資當事人拒絕自動化決策之權利，並新增第 37 條之 2，就該權利之行使作出細部規定；此一版本草案並未就自動化決策之告知作出特別規範。

（七）新加坡個人資料保護法

新加坡個人資料保護法並未明文賦予當事人針對個人資料的停止利用或拒絕權。

然而，由於新加坡個人資料保護法將「當事人同意（包含視為同意）」列為組織蒐集、利用或揭露個人資料的合法

[52] 개인정보보호위원회，「개인정보 보호법」일부개정법률(안)입법예고（2021.01.06），https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS061&mCode=C010010000&nttId=7059#LINK。

[53] 개인정보보호위원회，디지털 시대 「개인정보 보호법」 개정안 국회제출（2021.09.28）https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7565#LINK。

要件之一[54]，並明文規範當事人有權隨時向組織撤回其針對蒐集、利用或揭露個人資料行為所表示之同意[55]，因此，在組織以「當事人同意」作為蒐集、利用或揭露個人資料之依據時，如當事人針對特定行為撤回其同意者，組織除符合個人資料保護法或其他法律之規定或受要求者外，即應依當事人撤回同意之意，停止蒐集、利用或揭露個人資料之行為[56]，此效果即與當事人拒絕權相仿。

四、法規比較

自上述比較法觀察，當事人對於合法利用其個人資料的行為之拒絕權應非絕對，各國有不同的法益取捨與規範方式。有允許當事人任意行使拒絕權者（例如韓國個人資料保護法），有針對特定處理個人資料之合法要件賦予拒絕權者（例如歐盟 GDPR），有針對特定行為賦予拒絕權者（例如歐盟 GDPR、美國加州 CCPA 及維吉尼亞州 CDPA），有針對特定風險賦予拒絕權者（例如日本個人資訊保護法），亦有未賦予拒絕權者（例如日本行政機關個人資訊保護法、新加坡個人資料保護法）。且即便賦予當事人對合法行為的拒絕權，該權利亦非絕對，比較法中仍對當事人的拒絕權定有例外，允許於特定要件下得拒絕當事人的權利行使。

由具體規範來看，比較法上對於商業營利中「非為履行契約所必要之」利用個資行為—例如歐盟 GDPR 中的行銷與自動化決策、美國加州 CCPA 中的出售或分享個人資料、美國維吉尼亞州 CDPA

[54] Singapore, PDPA ,§13, " An organisation shall not, on or after the appointed day, collect, use or disclose personal data about an individual unless —(a) the individual gives, or is deemed to have given, his consent under this Act to the collection, use or disclosure, as the case may be; or (b) the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or any other written law."

[55] Singapore, PDPA ,§16(1), "On giving reasonable notice to the organisation, an individual may at any time withdraw any consent given, or deemed to have been given under this Act, in respect of the collection, use or disclosure by that organisation of personal data about the individual for any purpose. "

[56] Singapore, PDPA ,§16(4), "Subject to section 25, if an individual withdraws consent to the collection, use or disclosure of personal data about the individual by an organisation for any purpose, the organisation shall cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless such collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or other written law."

中的精準廣告、出售個人資料與為作成對該消費者發生法律效力或類似重大效果之決定所為的剖析—給與當事人較多保障，企業似無從對抗當事人拒絕權的行使，此與我國個資法之精神相仿，惟我國個資法僅對於利用個人資料「行銷」之行為，賦予當事人絕對的拒絕權（第 20 條第 2 項）。

除此之外，當蒐集機關為執行公務或為公益目的而利用個人資料時，歐盟 GDPR 雖賦予當事人拒絕權，但蒐集機關即控管者如能證明其具有優勢利益之正當理由，或為建立、行使或防禦法律請求所需者，即構成得以對抗當事人拒絕權的例外；韓國個人資料保護法雖同樣賦予當事人拒絕權，但若公務機關將因此無法執行法定職務時，仍可拒絕當事人的權利行使；我國個資法則未就公務機關執行法定職務之行為或公務機關與非公務機關為增進公共利益所必要之行為，賦予當事人得以拒絕之權利。

又在將個人資料用於科學、歷史研究或統計目的之情形，歐盟 GDPR 亦賦予當事人拒絕權，但如該行為係為公共利益之任務執行者，當事人拒絕權即受限制；我國個資法則未對於蒐集機關的研究行為賦予當事人拒絕權（但研究行為須受法定目的限制，且資料經處理後或依揭露方式須無從識別當事人）。

至於當法律規定「正當利益」作為合法利用個人資料的合法要件之一時，歐盟 GDPR 賦予當事人拒絕權，但控管者如能證明其具有優勢利益之正當理由，或為建立、行使或防禦法律請求所需者，即構成得以對抗當事人拒絕權的例外；韓國個人資料保護法則是未將正當利益列為個人資料處理者得對抗當事人拒絕權之事由，是即便個人資料處理者之正當利益明顯優於當事人權利（此為韓國個人資料保護法第 15 條第 1 項第 6 款之要件），當事人仍得對個人資料處理者基於該正當利益利用個人資料之行為行使拒絕權；我國個資法則是未將「正當利益」列為公務機關或非公務機關合法蒐集、處理或利用個人資料之合法要件。

各國個資法規關於本議題之比較表格整理如下：

表 1、各國拒絕權相關規範比較表

國家		權利內容	法源依據	位階
臺灣		下列情形下，個資當事人得就其個人資料行使請求停止蒐集、處理或利用之權利： (1) 個人資料正確性有爭議者； (2) 個人資料蒐集之特定目的消失或期限屆滿時； (3) 違反本法規定蒐集、處理或利用個人資料者。	個人資料保護法第 3 條第 4 款、第 11 條第 2 項至第 4 項	法律
歐盟		1、控管者基於下列合法要件處理個人資料時，個資當事人得以其自身特定狀況為由，拒絕處理，惟控管者得基於更重大之利益而繼續處理： (1) 執行公益任務或行使公權力所必要； (2) 控管者之正當利益所必要。 2、為直接行銷而處理個人資料時，個資當事人得隨時拒絕處理。	GDPR§21	法律
美國	加州	1、消費者得隨時要求業者不得將其個人資料販售或分享予第三方。 2、業者將消費者個人資料販售或分享予第三方後，該第三方未明確通知消費者並給與其行使拒絕販售權之機會前，不得將該個人資料再行販售或分享。	CCPA, amended by CPRA § 1798.120	法律

國家		權利內容	法源依據	位階
	維吉尼亞州	消費者有權拒絕業者為下列目的處理其個人資料： (1) 精準廣告； (2) 販售個人資料； (3) 為決策目的進行剖析，且該決策對消費者有法律性或類似重大影響。	CDPA § 59.1-573(A)(5)	法律
日本		1、如個資處理者違法蒐集或處理個人資料，個資當事人得要求個資處理者停止利用其個人資料。 2、如個資處理者違法向第三方提供個人資料，個資當事人得要求個資處理者停止向該第三方提供。	個人資訊保護法§30	法律
韓國		1、個資當事人得要求個資處理者停止（정지）處理其個人資料。 2、於下列情形，處理者得拒絕停止處理： (1) 遵守法定義務所必要； (2) 保護他人生命、身體、財產或其他利益所必要； (3) 公務機關執行法定職務所必要； (4) 履行與各自當事人間契約所必要，且個資當事人未明確表示解除契約。 3、個資處理者依個資當事人要求停止處理個人資料時，應立即採取銷毀個資等必要措施。	個人資料保護法§37	法律

國家	權利內容	法源依據	位階
新加坡	新加坡個資法規無個資當事人得拒絕處理其個資之明文規範。	-	-

五、修法需求分析

承繼上述法規比較，以下將由「當事人對機關基於合法要件之拒絕權」與「當事人對機關合法目的之拒絕權」，評估我國個資法增列當事人拒絕權之需求。

其中，雖然本議題並非探討個資法第 6 條、第 15 條、第 16 條、第 19 條、第 20 條規範之合法要件是否妥適，然而，對於合法行為不賦予當事人拒絕權之前提，應係該合法行為確實為正當、重要之目的，且符合比例原則，因此本報告在檢視個資法各款蒐集、處理與利用個人資料的合法要件時，將一併評估該合法要件的適當性，以作為判斷須否修法賦予當事人拒絕權之基礎[57]。

（一）特種個資合法要件檢視

1、 法律明文規定

於法律明文規定時，公務機關或非公務機關得蒐集、處理或利用當事人之特種個人資料（個資法第 6 條第 1 項但書第 1 款）。

此規範乃因個資法具有普通法性質，當其他法律基於正當、重要目的而對特種個人資料之蒐集、處理或利用另有規定時，自應依該特別法為據。是在蒐集機關依法律明文規定，合法蒐集、處理或利用特種個人資料時，除非該法另有規定，否則應不宜於個資法中賦予當事人拒絕之權，以免減損該法律目的之達成。

[57] 如同前述，「當事人（書面）同意」之合法要件不在本議題討論之列。

2、 公務機關執行法定職務必要範圍

公務機關於執行法定職務之必要範圍內，得蒐集、處理與利用特種個人資料（個資法第 6 條第 1 項但書第 2 款前段）。

此規範係為確保公務機關得有效依法執行其職務，具有重要公益目的；且公務機關受「必要原則」之限制，倘處理或利用行為逾越蒐集目的必要範圍即構成違法，當事人自可對該違法行為請求公務機關停止處理、利用。因此，限制當事人對公務機關在執行法定職務之必要範圍內處理、利用特種個人資料之拒絕權，應不違反比例原則，未侵害憲法對基本權的保障。

比較法上，前述韓國個人資料保護法第 37 條第 1 項允許當事人對處理個人資料之行為行使拒絕權（未區分該行為係合法或違法），但同條第 2 項第 3 款「公務機關如未處理個人資料將無法執行其他法律所定之職務」之例外事由，即令公務機關得為法定職務之必要而拒絕當事人的權利行使，此法律適用效果與我國個資法類似，但其條文則是「以當事人得行使拒絕權為原則」，「公務機關得與之對抗為例外」，此立法例的實質意義或將體現於當由司法機關判斷當事人的請求是否有理由時（判斷公務機關是否逾越必要範圍而蒐集、處理或利用個人資料），在我國由於個資法第 11 條第 4 項以「違法」為當事人請求停止行為的要件，似將由當事人對「公務機關逾越必要範圍而違法」負舉證責任，但在韓國則因前述規定，似須由主張有利於己之例外事由的公務機關對其「未逾越必要範圍」承擔舉證之責。

另歐盟 GDPR 第 21 條第 1 項允許當事人對執行公務而處理個人資料之行為行使拒絕權，但如控管者能證明

其行為相較當事人之利益、權利或自由具有優勢正當理由時，即可免除滿足當事人拒絕權之義務，此規範亦將舉證責任劃由控管者負擔，減輕當事人的救濟成本，對當事人的自主權行使較有保障。

本報告認為，公務機關基於國家高權地位，為執行法定職務而蒐集、處理與利用人民的個人資料，固蘊有權力不平等之性質，歐盟及韓國於個資法中賦予當事人拒絕權，並由公務機關承擔「優勢公益」或「未逾越必要範圍」之舉證責任，乃強化當事人隱私保護及資訊自主權之制度設計。況特種個資敏感性較高，當事人對其隱私期待及自主權水平亦應較高；而我國實務上所認之公務機關「法定職務」範圍，亦含組織法所定之掌理事項，其具體範圍相對較有彈性，如就特種個資賦予當事人拒絕權，自屬為個資當事人之隱私權及資訊自主權提供更高保護之舉。然從另一面向觀察，公務機關既係依法律執行職務，則其必要範圍內之個資蒐集、處理與利用，應可認已由立法者事前概括衡平公務機關執行職務之公益，與對人民（當事人）資訊隱私權及自主權之潛在限制。是否需參考歐盟及韓國法制，賦予當事人於事後在個案中之拒絕權，則涉我國社會及文化環境中，公務機關執行法定職務之安定性與當事人資訊隱私權及自主權更高保護之調和。又考量我國個資法居於個資蒐集、處理及利用之普通法地位，公務機關執行職務如致使某一特種個資面臨較高風險，自可通過制定特別法之方式，就該特定職務之執行，賦予當事人事後個案中之拒絕權，對公務機關課以證明「優勢公益」、「未逾越必要範圍」之較高義務。故從適足保護當事人資訊隱私權及自主權，並兼顧公務機關執行法定職務安定性之視角，可認現階段尚不需於個資法中，針對公務機關執行法定職務必要

範圍內蒐集、處理與利用特種個資，賦予當事人普遍性拒絕權。

3、非公務機關履行法定義務必要範圍

非公務機關於履行法定義務之必要範圍內，得蒐集、處理與利用特種個人資料（個資法第 6 條第 1 項但書第 2 款後段）。

此規範係為確保非公務機關得有效履行其受法律要求之義務，目的洵屬正當，若賦予當事人對非公務機關為履行法定義務而蒐集、處理或利用個人資料之拒絕權，將使非公務機關陷於相斥義務的兩難，有礙於該特別法課予受規範之蒐集機關義務的目的達成。

4、當事人自行公開或其他已合法公開之特種個人資料

公務機關或非公務機關對於當事人自行公開或其他已合法公開之特種個人資料，得蒐集、處理或利用之（個資法第 6 條第 1 項但書第 3 款）。

此規範目的依其立法理由係因「隱私已無被侵害之虞」（參個資法第 6 條立法理由），而允許蒐集機關蒐集、處理或利用當事人自行公開或已合法公開之特種個人資料。

然而，當事人自行公開個人資料之目的不一，法律規定應公開個人資料之目的亦有該法追求之正當目的，惟在現行個資法適用下，機關蒐集、處理或利用已公開之個人資料，其自身之特定目的並未限制須與當事人自行公開之目的或法律規定應公開之目的相符，立法理由考量此時「（資訊）隱私權」亦無被侵害之虞，固非無見，但由「資訊自主權」的角度來看，當事人控制其個人資料被如何處理或利用之權利恐將受有減損。

且我國個資法將本款列為得蒐集、處理與利用特種個人資料之要件，蒐集機關僅以本款事由即可蒐集、處理與利用特種個人資料，無須考量其他行為依據（例如公務機關是否為執行法定職務、非公務機關是否為履行法定義務），似亦與憲法保障隱私權的精神—為重要目的始得以法律限制—有所扞格。

比較法上，歐盟 GDPR 第 9 條第 1 項先禁止控管者處理高度敏感的特種個人資料[58]，再於同條第 2 項列舉數款情形得免除第 1 項的禁止，其中，第 e 款即將「明顯由當事人自行公開的個人資料之處理行為」列為免除禁止事由之一[59]。然而，本條之目的係在規範何種情形下的特種個人資料可例外被處理，而非列舉控管者得處理個人資料之合法要件，因此，即便該特種個人資料已明顯由當事人自行公開而不受 GDPR 禁止處理，控管者仍需符合 GDPR 第 6 條列舉的合法要件之一，始得合法處理該特種個人資料。此立法即對當事人資訊自主權較有保障，不致因自行公開而再也無從限制控管者處理其個人資料。

因此，在現行個資法下，蒐集機關若無從適用其他合法要件，僅以本款作為蒐集、處理或利用個人資料之依據，似宜適當賦予當事人拒絕該行為的權利，以平衡保障當事人的自主權。

5、研究條款

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

[58] EU, GDPR, §9(1), "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

[59] EU, GDPR, §9(2), "Paragraph 1 shall not apply if one of the following applies: …(e) processing relates to personal data which are manifestly made public by the data subject…".

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時，得蒐集、處理與利用特種個人資料（個資法第6條第1項但書第4款）。

此規範係為促成公務機關與學術研究機構的「醫療、衛生或犯罪預防」此三種特別重要之公益目的達成，在為「統計或學術研究」而有必要時，例外得蒐集、處理及利用特種個人資料，並限於當該特種個人資料「經提供者處理後」或「經蒐集者依其揭露方式」無從識別特定之當事人時，始得為之。

雖然立法理由認為，資料既已經過去識別化，「應無侵害個人隱私權益之虞」，然而，資訊隱私與資訊自主同為憲法保障人民隱私權之重要內涵，資料去識別化雖可有效保護當事人之隱私[60]，但該行為仍對當事人的資訊自主控制之權有所干預[61]。

不過，本研究條款畢竟出於重要公益目的考量，在符合比例原則的限度內，排除當事人拒絕之權應無不可。

在公務機關或學術研究機構作為「提供（利用）者」的情形，本款規定允許其提供「未經去識別」之特種個人資料予蒐集者，則蒐集者是否在揭露統計或研究結果時，確實達到資料去識別化之效果，似已非提供者所能控管，倘一概不許當事人拒絕將未經去識別之特種個人資料對外提供，對於當事人資訊自主權的保障恐嫌不足。

又在公務機關或學術研究機構作為「蒐集者」之情形，若特種個人資料經過提供者處理後，已無從直接識別或與其他資料對照、組合、連結而識別特定當事人時，公務機關或學術研究機構取得的資料已非個人資料，從

[60] 至於具體情形的資料去識別化程度如何，是否能有效達到匿名效果，此為另一層次問題。

[61] 尤因公務機關或學術研究機構適用本款情形，恐多係間接蒐集當事人個人資料，倘符合個資法第9條第2項各款規定之一而免除告知義務時，當事人可能無從知悉。

現實面來看，無從讓當事人「就其個人資料」行使拒絕權。然而，本款規定並未明文要求提供者將資料處理至無法間接識別之程度，並允許公務機關或學術研究機構取得「未經去識別化」之特種個人資料，僅在事後如欲揭露其統計或研究結果時，須確保該結果無從識別特定之當事人。則在公務機關或學術研究機構保有當事人之特種個人資料（以供日後、持續統計或研究之用）期間，仍有識別當事人之相當可能。此時，當事人對其個人資料的資訊隱私、自主權之利益是否均劣後於公務機關或學術研究機構為「醫療、衛生或犯罪預防」之統計或學術研究利益，似無法一概而論[62]。

若公務機關基於法定職務之執行而有必要，其追求之利益優於當事人之利益應較無爭議，但此時公務機關應適用個資法第 6 條第 1 項但書第 2 款前段作為合法要件。惟當公務機關非為執行法定職務時，或學術研究機構為統計或學術研究時，即便係為醫療、衛生或犯罪預防之目的，何以其利益必然大於當事人之利益，而可限制當事人之拒絕權，恐有斟酌餘地[63]。

比較法上，歐盟 GDPR 並未將研究條款列為第 6 條控管者處理個人資料之合法要件，而是於第 89 條第 1 項規定研究目的之安全維護措施要件，即控管者須符合第 6 條所列情形之一（例如公務機關執行公務、非公務機關履行與當事人間之契約、取得當事人同意等），並對個

[62] 此處須留意的是，立法者將本研究條款列為公務機關蒐集、處理與利用特種個人資料的合法要件之一，與前述「公務機關執行法定職務所必要」之合法要件似為擇一關係，則在具體情形，當公務機關為執行法定職務而有統計資料之必要時，似以個資法第 6 條第 1 項但書第 2 款為據即可，不受本款「特定重要公益目的」以及「資料去識別化」的限制，反之，即便與法定職務無關，公務機關亦可主張本款事由而蒐集、處理與利用特種個人資料，是否妥當不無疑問。

[63] 況學術研究機構如基於「經當事人書面同意」而直接向當事人蒐集特種個人資料時，當事人知悉且可經由撤回同意來拒絕學術研究機構利用其特種個人資料，則在當事人事先不知情的間接蒐集特種個人資料情形，於當事人知情後反因本款事由而無從拒絕，似有輕重失衡之虞。

人資料採取適當的安全維護措施，始得為科學或歷史研究，或統計目的處理個人資料。此時，當事人依第 21 條第 6 項規定，得向控管者行使拒絕權，但如控管者係為公共利益之任務執行而為研究，則可例外以之對抗當事人的權利行使。

此規定先以「合法要件」限縮控管者為研究目的處理個人資料之行為，再搭配當事人得表示拒絕以保障其資訊自主權，另輔以公益優勢但書以確保公益目的的達成，但將舉證責任分配由主張公益必要性的控管者承擔，較之我國個資法似更能兼顧研究目的與當事人權利的平衡。

是在本研究條款情形，我國個資法如能適當賦予當事人拒絕權，並由蒐集或提供其特種個人資料之公務機關或學術研究機構，承擔優勢公益及不將資料去識別之必要性的舉證之責，應較能兼顧當事人的權利保障，更可消弭本款適用的實務爭議。

6、 必要協助條款

公務機關或非公務機關在「協助公務機關執行法定職務」或「協助非公務機關履行法定義務」的必要範圍內，得蒐集、處理與利用特種個人資料（個資法第 6 條第 1 項但書第 5 款）。

本款特別將「協助」行為列為要件，應是排除「受委託」蒐集、處理或利用特種個人資料之行為（否則依個資法第 4 條「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關」之規定適用法律即可），由民國 104 年修正公布新增本款之立法理由「對於合法保有特種資料之機關，基於協助其他公務機關執行法定職務或其他非公務機關履

行法定義務所必要，而提供該特種個人資料予該等公務機關或非公務機關，則未有規定」可知，增列本款之目的係為讓「已保有」特種個人資料之機關，可合法提供（利用）該資料予其他公務機關或非公務機關，以協助其執行法定職務或履行法定義務，其本質應為「目的外利用」特種個人資料之行為（雖然個資法第 6 條並未區分特種個人資料的目的內或目的外利用要件）。

本款規定並非課予蒐集者「必須」協助而提供特種個人資料之義務。實務運作中，本款並不要求蒐集者負有依其他法律應予提供資料之義務，而是以資料收受機關執行法定職務或履行法定義務之必要，作為判斷蒐集機關目的外利用正當性之依據。因此，若個資法在此賦予當事人拒絕權，自可敦促蒐集者謹慎評估「為協助而提供資料」之適當性，平衡當事人的權利保障。

然考量本款規定係為解除特種個人資料的利用禁止，使蒐集者不因提供特種個人資料予公務機關或非公務機關而受到處罰（刑事責任、行政責任）或不利（民事責任）。於公務機關之「法定職務」或非公務機關之「法定義務」已由立法者事前概括衡平相關法律所涉之公益，與對人民（當事人）資訊隱私權及自主權之潛在限制之前提下，似可認基於必要協助而目的外利用個資之行為乃落實立法者價值衡量之必要舉措，而得受較寬鬆之檢視，現階段於個資法中，尚不需就此賦予當事人拒絕之權。

（二）一般個資合法要件檢視

1、法律明文規定

非公務機關基於法律明文規定，得蒐集、處理（並於蒐集目的範圍內利用）一般個人資料（個資法第 19 條第 1 項第 1 款、第 20 條第 1 項本文）。

如同前述，此規範乃因個資法具有普通法性質，當其他法律基於正當、重要目的而對個人資料之蒐集、處理或利用另有規定時，自應依該特別法為據，應不宜於個資法中賦予當事人拒絕之權。

2、 公務機關執行法定職務必要範圍

公務機關於執行法定職務之必要範圍內，得蒐集、處理（並於蒐集目的範圍內利用）一般個人資料（個資法第 15 條第 1 款、第 16 條本文）。

如同前述（特種個資的合法要件檢視），此規範係為確保公務機關得有效依法執行其職務，具有重要公益目的，限制當事人對公務機關在執行法定職務之必要範圍內處理、利用個人資料之拒絕權，應不違反比例原則。而考量當事人資訊隱私權及自主權保護與公務機關執行法定職務安定性之衡平，現階段應尚不需於個資法中，針對公務機關執行法定職務必要範圍內蒐集、處理與利用一般個資，賦予當事人普遍性拒絕權。

3、 與當事人有契約或類似契約之關係

非公務機關如與當事人間有契約或類似契約之關係，得於履約、締約的必要範圍內蒐集、處理（並於蒐集目的範圍內利用）當事人的一般個人資料（個資法第 19 條第 1 項第 2 款、第 20 條第 1 項本文）。

此規範係為使蒐集機關與當事人間有效締約或履約，符合當事人追求之契約利益，如任當事人於契約期間行使拒絕權，將徒增雙方契約履行之困擾。況倘當事人於

磋商階段決定不欲締約，或於履約期間終止契約，此時即可視是否構成「特定目的消失」而依個資法第 11 條第 3 項行使權利，並未限制當事人的權利保障。

4、當事人自行公開或其他已合法公開之一般個人資料

非公務機關得蒐集、處理（並於蒐集目的範圍內利用）當事人自行公開或其他已合法公開之一般個人資料，（個資法第 19 條第 1 項第 3 款、第 20 條第 1 項本文）。

此規範目的依其立法理由係因當事人自行公開或已合法公開之個人資料「已無保護之必要」（參個資法第 19 條立法理由），而允許蒐集機關蒐集、處理或利用當事人自行公開或已合法公開之個人資料。

然如前述（特種個資的合法要件檢視），在現行個資法適用下，蒐集機關蒐集、處理或利用已公開之個人資料，其自身之特定目的並未限制須與當事人自行公開之目的或法律規定應公開之目的相符，當事人的「資訊自主權」是否在此「已無保護之必要」，恐有探究空間。

是在蒐集機關無從適用其他合法要件，僅以本款作為蒐集、處理或利用個人資料之情形，似宜適當賦予當事人拒絕該行為的權利，以平衡保障當事人的自主權。

5、研究條款

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時，得蒐集、處理（並於蒐集目的範圍內利用）一般個人資料（個資法第 19 條第 1 項第 4 款、第 20 條第 1 項本文）。

如前所述（特種個資合法要件檢視），此規範允許學術研究機構取得「未經去識別化之個人資料」，僅在

事後如欲揭露其統計或研究結果時，須確保該結果無從識別特定之當事人。則在學術研究機構保有當事人之一般個人資料（以供日後、持續統計或研究之用）期間，當事人對其個人資料的資訊隱私、自主權之利益是否均劣後於學術研究機構為公共利益之統計或學術研究利益，難以一概而論。

誠然，學術研究之公益目的有其重要價值，但個資法如能在此適當賦予當事人拒絕權，並由學術研究機構證明蒐集、處理該當事人之一般個人資料，對其研究之優勢公益目的達成具有必要性，應較能兼顧當事人權利的保障。

6、 公益條款

非公務機關為增進公共利益所必要者，得蒐集、處理（並於蒐集目的範圍內利用）一般個人資料（個資法第 19 條第 1 項第 6 款、第 20 條第 1 項本文），本款原於民國 99 年修正公布條文為「與公共利益有關」，嗣於民國 104 年 12 月 30 日修正公布為「為增進公共利益所必要」，立法理由係因當蒐集機關為公益目的而處理或利用個人資料時，應限於必要之範圍，是酌為文字修正。

本款條文並未限定適用此公益條款之非公務機關類型或所欲增進之公共利益具體內容（相較之下，個資法第 9 條第 2 項第 5 款規定「大眾傳播業者基於新聞報導之公益目的而蒐集個人資料」，可免除向當事人揭露法定資訊的告知義務，即限縮適用主體為基於新聞報導之公益目的的大眾傳播業者），是任何非公務機關均有可能為各類公益目的而依據本條款蒐集、處理及利用個人資料。

然而，「公共利益」畢竟為一典型的不確定法律概念，並有高低程度不同之別，且非公務機關類別多元，所從事之業務亦多種多樣，非公務機關如何判斷或主張其蒐集、處理與利用個人資料之行為，係與公共事務有關而為增進公共利益所必要，恐易生爭議。個資法如能適當在此賦予當事人拒絕權（立法上可搭配「優勢公益」的例外），應較能緩和由蒐集機關單方主張公益條款即蒐集、處理與利用當事人一般個人資料所造成的衝突。

7、個人資料取自於一般可得之來源

如本節二(五)所述，若個人資料取自於一般可得之來源者，非公務機關得蒐集、處理（並於蒐集目的範圍內利用），但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限（個資法第 19 條第 1 項第 7 款、第 20 條第 1 項本文），此規定即謂當事人「禁止處理或利用個人資料」之通知，將使蒐集機關不得再繼續處理或利用其個人資料，其效果等同拒絕權之行使。

8、對當事人權益無侵害

公務機關與非公務機關於不侵害當事人權益時，得蒐集、處理（並於蒐集目的範圍內利用）一般個人資料（個資法第 15 條第 3 款、第 16 條本文、第 19 條第 1 項第 8 款、第 20 條第 1 項本文）。此規範首見於民國 84 年制定公布的電腦處理個人資料保護法第 7 條第 3 款，即公務機關「對當事人權益無侵害之虞者」，得蒐集、電腦處理與利用個人資料，立法理由為「鼓勵資料流通與保護個人資料之平衡」。嗣本款於民國 99 年修正公布之個

資法第 15 條第 3 款刪除「之虞者」三字，以求公務機關蒐集、處理個人資料之要件明確。

後於 104 年修正公布之個資法中，立法者於第 19 條第 1 項第 8 款增列本要件作為非公務機關得蒐集、處理與利用一般個人資料之依據，立法理由乃基於非公務機關倘無該款要件可資適用，將致實務上於特定情形欲蒐集個人資料「反成窒礙難行」，往往須另行取得當事人之同意，不僅造成當事人困擾，亦造成各機關沉重之行政作業負擔，爰增訂此款規定。

本款作為公務機關與非公務機關得以蒐集、處理與利用一般個人資料之合法要件是否恰當，在此不論[64]，惟由於本款單以該行為對當事人權益有無侵害作為考量，未將該行為是否對蒐集機關具有正當利益納入要素，則似宜賦予當事人適當之拒絕權，降低當事人若認為該行為侵害其權益，尚須向蒐集機關爭執之成本，而許當事人任意拒絕蒐集機關依本款合法要件繼續處理或利用其個人資料。

（三）一般個資合法目的外利用要件檢視

1、法律明文規定

公務機關與非公務機關皆可在法律明文規定時，於原始蒐集目的之外利用一般個人資料（個資法第 16 條但書第 1 款、第 20 條第 1 項但書第 1 款）。

[64] 本款所稱「權益」為何並不明確，如排除隱私權，較難想像蒐集、處理與利用個人資料的行為，將侵害當事人除隱私權（含資訊自主權）以外的何種權利或其他利益，則公務機關或非公務機關是否皆以此款為據，即可不適用其他合法蒐集、處理一般個人資料的合法要件，不無疑問。惟若此處權益不排除隱私權，則因個人資料的蒐集、處理及利用行為，本質上應視為對隱私權的干預，僅在法律允許範圍內始得為之，若認為本款包含「對當事人隱私權（資訊自主權）無侵害」，由於對隱私權不構成侵害的原因可能出於當事人同意、可能係因當事人自行公開資料，然此兩者皆有合法要件可資適用（個資法第 15 條第 2 款、第 19 條第 1 項第 5 款、第 3 款），則本款另概括列入「對當事人隱私權（資訊自主權）無侵害」之合法要件，恐造成判斷上的困難。

此規範目的係為確保作為普通法之個資法不致阻礙特別法律所欲追求的重要目的，是在蒐集機關依法律明文規定而利用個人資料時，即便與原本蒐集資料之目的並不相符，仍不宜於個資法中賦予當事人拒絕之權，以免減損該法律目的之達成。

2、國安條款

公務機關為維護國家安全所必要，得於原始蒐集目的之外利用一般個人資料（個資法第 16 條但書第 2 款前段）。

此規範係為國家安全之維護，乃重要之公益目的，若任當事人對公務機關的必要行為行使拒絕權，勢將危害國家安全的維護，應不適當。

3、公益條款

公務機關或非公務機關為增進公共利益所必要，得於原始蒐集目的之外利用一般個人資料（個資法第 16 條但書第 2 款後段、第 20 條第 1 項但書第 2 款）。

此規範追求公益目的之達成，尚屬正當、重要，實務上多適用於保有個人資料之機關為協助公務機關執行法定職務，而於原始蒐集目的之外將個人資料提供予該公務機關，或為該公務機關利用。例如交通部公路總局將已黏貼 eTag 車輛過戶後之新車主聯絡電話，提供予交通部國道高速公路局，以利後者執行「徵收國道通行費」之法定職務[65]、私立大學將學生個人資料提供予司法機關以執行偵辦刑事案件之法定職務[66]、電信公司在寄送予客戶之帳單內或信封上，配合政府機關刊載政令宣導[67]等。

[65] 見法務部 107 年 9 月 5 日法律字第 10703513330 號函。
[66] 見法務部 107 年 5 月 15 日法律字第 10703506760 號函。
[67] 見法務部 107 年 7 月 3 日法律字第 10703507550 號函。

然如前述，「公共利益」屬於不確定法律概念，並有高低程度不同之別，且既為「目的外」利用個人資料，對當事人就其個人資料「自主控制之合理期待」的影響更鉅，個資法如能適當在此賦予當事人拒絕權（立法上可搭配「優勢公益」的例外），應較能緩和當事人個人資料由蒐集機關單方主張公益條款，即在原始蒐集目的之外另為利用所造成的衝突。

4、為免除當事人之生命、身體、自由或財產上之危險

公務機關或非公務機關為免除當事人之生命、身體、自由或財產上之危險，得於原始蒐集目的之外利用一般個人資料（個資法第 16 條但書第 3 款、第 20 條第 1 項但書第 3 款）。

此規範目的係為保護個資當事人本人的重大法益，且依其性質似多為一次性的目的外利用個人資料行為（例如為釐清行方不明兒童可能行蹤，將兒童戶籍、親等關係及入出境等資料提供查訪兒童的社政主管機關[68]；戶政事務所將失蹤個案當事人及其家屬洽辦戶政業務留存之聯絡電話，提供警察機關以查尋失蹤人口[69]），是當蒐集機關依據本款為目的外利用個人資料時，應無必要賦予當事人拒絕權。

5、為防止他人權益之重大危害

公務機關或非公務機關為防止他人權益之重大危害，得於原始蒐集目的之外利用一般個人資料（個資法第 16 條但書第 4 款、第 20 條第 1 項但書第 4 款）。

此規範目的係為保護個資當事人以外之人，防止其權益受有重大危害，且其性質亦應多為一次性的目的外

[68] 見法務部 105 年 11 月 11 日法律字第 10503515840 號函。
[69] 見國家發展委員會 108 年 1 月 22 日發法字第 1080000958 號函。

利用個人資料行為（例如戶政事務所提供無自理能力患者之親屬資料予公立醫院，供醫院聯繫處理相關事宜，以防止患者生命、身體之重大危害[70]），是當蒐集機關依據本款為目的外利用個人資料時，亦應無必要賦予當事人拒絕權。

6、研究條款

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（個資法第 16 條但書第 5 款、第 20 條第 1 項但書第 5 款）

此規範分別作為公務機關及非公務機關得於「原始蒐集目的之外利用」一般個人資料之依據，使該機關得將已保有之一般個人資料合法提供予其他公務機關或學術研究機構。

此時，本款規定允許該保有一般個人資料之公務機關或非公務機關將「未經去識別」之個人資料對外提供，則蒐集者是否在揭露統計或研究結果時，確實達到資料去識別化之效果，似已非提供者所能控管。

由於目的外利用個人資料之行為已對當事人的資訊自主合理期待造成干預，倘尚不許當事人拒絕將「未經去識別」之個人資料對外提供，對於當事人資訊自主權的保障恐嫌不足。

是如個資法在此能適當賦予當事人拒絕權，並由已保有其一般個人資料之公務機關或非公務機關承擔優勢公益及不將資料去識別之必要性的舉證之責，應較能兼顧當事人的權利保障。

[70] 見法務部 104 年 8 月 20 日法律字第 10403510420 號函。

7、有利於當事人權益

公務機關或非公務機關在有利於當事人權益時，得於原始蒐集目的之外利用其個人資料（個資法第 16 條但書第 6 款、第 20 條第 1 項但書第 7 款）。

此規範目的為何並不明確，民國 84 年制定公布之電腦處理個人資料保護法，於第 8 條但書第 8 款將此列為公務機關得於特定目的外利用個人資料之事由（其後本款於 99 年修正公布之個資法移列於現行第 16 條但書第 6 款），其立法理由僅為「目的外利用係...有利於當事人權益...應予准許」；民國 104 年修正公布之個資法於第 20 條第 1 項但書第 7 款增列本款為非公務機關得於特定目的外利用個人資料之事由，其立法理由亦僅為「若特定目的外利用有利於當事人權益者，應可為特定目的以外之利用」。

如以文義理解，本款規定係為讓當事人之權益有獲得更佳利益之機會，即便目的外利用個人資料之行為可能逾越當事人合理期待的範圍，但既然該行為有利於當事人權益，立法者即認為應允許蒐集機關為該增進當事人權益之行為。

然而，既然本款規定單以該行為是否有利於當事人權益為斷，並不考量蒐集機關對該利用行為是否具有正當利益，則倘當事人不願享受該權益，應無不許之理，個資法宜對本款事由適當賦予當事人拒絕權，以確保當事人對其隱私自主與其他權益之取捨享有選擇之權。

（四）合法目的之拒絕權

比較法上規範當事人對於蒐集機關基於合法目的之行為的拒絕權，多以商業營利行為為標的（例如行銷、精準廣告、

出售個資、剖析等），所考量者應係此類行為以個人資料作為營利方式，公益價值較低，當事人的資訊自主權應有更值得保護之利益。

我國個資法亦對非公務機關利用個人資料行銷之行為，賦予當事人無條件的拒絕之權（個資法第 20 條第 2 項），但除此之外，是否應於個資法中增列其他合法行為作為當事人拒絕之標的，似非一蹴可及。蓋正面表列各種目的之行為，於立法上有其難處，不僅須詳究是否掛一漏萬，亦須充分評價對不同行為取捨之理由，更應兼顧蒐集機關合法行為的利益與當事人利益的權衡，以符合個資法「促進個人資料合理利用」的本意。

以目前較具代表性之歐盟個資法為參考，GDPR 中，當事人得拒絕的合法目的包含行銷與研究，前者於我國個資法亦有規範，後者為前述宜賦予當事人適當拒絕權的修法建議，已與 GDPR 規範有所匹配。惟 GDPR 尚於第 22 條賦予當事人對自動化決策的拒絕權（美國加州 CCPA 與韓國個人資料保護法亦有意新增規範），此為我國個資法所無，本報告認為，考量數位時代下的資料蒐集、探勘與分析技術日新月異，各種人工智慧、演算法與大數據的搭配應用層出不窮，自動化決策將是蒐集機關創造資料價值的重要工具。此時，倘當事人對蒐集機關的自動化決策全無置喙餘地，恐難以避免類似資訊歧視、區別待遇等對當事人不公平之情事發生。據此，我國個資法應可參酌歐盟 GDPR 之精神，適當增加當事人對於自動化決策行為拒絕權之原則與例外，除保障當事人權益外，更能作為蒐集機關有效運用自動化決策之依據。

六、本節結論

綜合本節比較研究，本報告認為，我國個資法宜就下列蒐集、處理與利用個人資料之合法要件，以及蒐集機關利用個人資料的自

動化決策行為，藉由原則與例外的法益價值安排，適當賦予當事人對蒐集機關表示拒絕之權，並調整舉證責任。

（一）在適用「當事人自行公開或已合法公開」的情形，蒐集機關倘無從適用其他合法要件，宜適當賦予當事人拒絕之權。

（二）在適用「研究條款」的情形，如資料提供者未先將資料去識別後提供，應許當事人拒絕，並由蒐集或提供個人資料之機關承擔優勢公益及不將資料去識別之必要性的舉證之責，較能兼顧當事人的權利保障。

（三）在適用「公益條款」的情形，考量其為不確定法律概念且有高低程度不同之別，個資法宜適當賦予當事人拒絕權，由蒐集機關承擔優勢公益的舉證責任，應較能緩和由蒐集機關單方主張公益條款即蒐集、處理與利用當事人個人資料所造成的衝突。

（四）在主張「對當事人權益無侵害」的情形，於本款單以該行為對當事人權益有無侵害作為考量，未將該行為是否對蒐集機關具有正當利益納入要素，則似宜賦予當事人適當之拒絕權，降低當事人若認為該行為侵害其權益，尚須向蒐集機關爭執之成本。

（五）在主張「有利於當事人權益」的情形，由於本款規定單以該行為是否有利於當事人權益為斷，並不考量蒐集機關對該利用行為是否具有正當利益，則倘當事人不願享受該權益，應無不許之理，個資法宜對本款事由適當賦予當事人拒絕權。

（六）參酌歐盟 GDPR 之精神，適當增加當事人對於自動化決策行為拒絕權之原則與例外。

第二節 當事人查詢或閱覽權

一、議題釐清

本議題源於「臺灣開放政府國家行動方案」中的承諾事項 1-3「強化數位隱私與個資保護」[71]，欲探究者為「現行個資法雖有規定當事人查詢或請求閱覽權，惟於數位經濟蓬勃發展下，是否可透過指引等方式，進一步釐清當事人在網路上從事之活動或行為所產生紀錄之查詢範圍等」。對此，本議題即須針對「個資當事人在網路上從事之活動或行為所產生之紀錄，是否有權向個資蒐集機關查詢或請求閱覽其個資是否正被運用，及查詢或請求閱覽其個資運用之範圍等」進行研議。

本議題之分析，包括三個層面。首先是「個資當事人在網路上從事之活動或行為所產生之紀錄」（以下簡稱「數位足跡」[72]）是否構成個人資料。若構成個人資料，則將檢視個資法上是否存在查詢或請求閱覽數位足跡之權利。若存在該權利，則進一步檢視行使該權利是否存有相關限制。以下將以此三個層面為基本架構，回顧並比較我國與外國相關立法規範。

二、我國個人資料保護法

（一）數位足跡是否構成個人資料

我國個資法第 2 條第 1 款將個人資料定義為「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」。個資法施行細則第 3 條進一步說明，所謂「以間接方式」識別，係指「保有該資料之公務或非公務機關僅以該資料不能直接識別，

[71] 臺灣開放政府國家行動方案，2021 年 4 月，頁 12-15。

[72] 應說明者係，「數位足跡」乃本報告為論述方便所使用之簡稱。然「數位足跡」自身並非法律概念，其範圍與所含資訊之類別，目前未見統一定義。

須與其他資料對照、組合、連結等，始能識別該特定之個人」。

據此，數位足跡並非我國個資法明文列舉之個人資料類別，但若數位足跡具有直接或間接識別性（即透過與其他資料對照、組合、連結等而實現識別），則屬於個資法所稱之個人資料。例如，若當事人於使用網路產品或服務時，可能會提供姓名、聯絡方式等資訊，網路產品或服務提供者得將蒐集之數位足跡與該等資訊相比對，從而將數位足跡連結到特定當事人[73]。

「間接識別」需考量的問題係，若資料蒐集機關並不掌握足以實現識別的其他資料，則所蒐集之資料是否仍屬於個人資料？由於數位足跡可由網路產品或服務提供者自動蒐集，且網路產品或服務之使用未必要求蒐集其他資訊，此一問題對於判定數位足跡是否屬於個人資料有相當重要性。

對此，我國個資法主管機關國家發展委員會（以下稱國發會）認為，「間接識別性」強調該資料可透過與其他資料對照、組合、連結而實現識別之「可能性」，並不要求控管者實際持有或能夠取得實現識別所需的其他資料[74]。據此，縱使數位足跡蒐集者並未完全掌握足以識別當事人之全部資料，只要數位足跡有可能用於識別當事人，即屬於個人資料。

（二）個資法上的查閱權

我國個資法第 3 條規定當事人得就其個人資料行使之資料權利，其中包括查詢或請求閱覽之權利，以及請求製給複製本之權利。依個資法第 10 條，公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。依個資法第 13 條，公務機關或非公務機關受

[73] 見法務部 104 年 10 月 23 日法律字第 10403513240 號函。
[74] 見國家發展委員會 109 年 7 月 24 日發法字第 1090015912 號函。

理當事人查詢、閱覽或製給複製本之請求後，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。

因此，在數位足跡具有直接或間接識別性的前提下，當事人得就其數位足跡向蒐集機關請求查詢閱覽，以及請求製給複製本。蒐集機關原則應於法定時限內准許其請求，答覆查詢、提供閱覽或製給複製本。

（三）查閱權之行使限制

依個資法第 10 條但書規定，於下列情形，當事人就其個人資料提出查詢、閱覽或製給複製本之請求後，蒐集機關無須答覆查詢、提供閱覽或製給複製本：(1)妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益；(2)妨害公務機關執行法定職務；(3)妨害該蒐集機關或第三人之重大利益。個資法施行細則第 18 條說明，所謂第三人之重大利益，係指有害於第三人個人之生命、身體、自由、財產或其他重大利益。據此，數位足跡之蒐集機關得以前開第三款，援用自身重大利益，拒絕當事人之查詢、閱覽或製給複製本之請求。

綜上所述，於我國個資法中，數位足跡在具有直接或間接識別性之前提下，屬於個人資料，個資當事人得就其行使查詢、閱覽或請求製給複製本之權利。蒐集機關亦得援引法定例外事由（包括自身之重大利益）拒絕當事人之請求。

三、外國立法例

（一）歐盟 GDPR

1、數位足跡是否構成個人資料

依 GDPR 第 4 條第 1 款，「個人資料」係指關於可識別或可得識別之自然人之任何資訊。所謂「可得識別之自然人」（identifiable natural person），係指可直接或間接被識別之人，包括可透過「網路識別碼」（online identifier）識別者[75]。

GDPR 自身並未就網路識別碼進行定義。但前言第 30 點指明，網路識別碼之來源包括資料當事人之裝置、應用程式、工具或通訊協定等，具體示例包括 IP 位址、cookie 識別碼、無線射頻辨識碼（RFID tag）等。網路識別碼之使用可能留下軌跡，而該等軌跡可用於剖析和識別個資當事人。若該等軌跡與獨特性識別碼或伺服器接收到的其他資料相結合，剖析和識別的可能性更高[76]。

是故，歐盟 GDPR 在立法過程中，即已考量透過數位足跡辨識個人當事人之可能性，並將與產生數位足跡密切相關之網路識別碼明文列舉為個人資料之一類。資料當事人之數位足跡，因與可識別之自然人相關，應落入個人資料之範圍。

2、GDPR 中的查閱權

GDPR 於第三章規範當事人權利，其中與本議題相關者為第 15 條的近用權（right of access）。依該條規範，個資當

[75] EU, GDPR, §4(1), 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;…"

[76] EU, GDPR, Recital 30, "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."

事人之近用權有三個面向：其一，當事人有權向控管者確認是否處理其個人資料。其二，控管者若處理其個人資料，個資當事人有權存取其個人資料及相關資訊，包括(1)處理之目的，(2)所涉個人資料之類型，(3)資料預期儲存期間或確定儲存期間之標準，(4)資料之揭露對象，(5)當事人請求更正、刪除、限制處理、拒絕處理以及向主管機關申訴之權利，(6)資料係自第三方取得時，資料來源之充分資訊，(7)資料是否用於自動化決策（包括剖析），若是，決策邏輯方面有實質意義的資訊、該等處理之重要性及預期結果，(8)資料傳輸至境外時，控管者採取的適當安全維護措施[77]。其三，控管者應就其處理之個人資料提供乙份副本，且對於電子方式提出近用權請求，原則應以通用電子形式提供副本[78]。

由 GDPR 第 15 條內容可知，個資當事人有權向控管者確認個人資料處理之相關資訊、存取其個人資料，並取得資料副本。由於數位足跡應屬個人資料，個資當事人應可就控管者所處理之數位足跡，向控管者行使第 15 條之近用權。在當事人之數位足跡用於剖析之情形，個資當事人得依據 GDPR 第 15 條第 3 項，要求控管者提供用作建立剖析檔案之輸入資

[77] EU, GDPR, §15(1), "The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."

[78] EU, GDPR, §15(3), "The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form."

料、剖析檔案之相關資訊，以及當事人所屬細分類別（segment）之細節[79]。

3、查閱權之行使限制

當事人依 GDPR 第 15 條行使近用權時，可能受有限制。首先，依 GDPR 第 15 條第 4 項規定，依同條第 3 項取得副本之權利不應對其他人之權利及自由有不利影響[80]。

前言第 63 點說明，此等他人之權利或自由包括營業秘密或智慧財產權，尤其是軟體著作權，但控管者不得基於對他人權利及自由之考量，拒絕向個資當事人提供一切（all）資訊。歐洲個人資料保護委員會（European Data Protection Board, EDPB）對此指出，某些情形下，基於對他人權利及自由有嚴重不利影響，控管者得考慮拒絕提供個人資料之副本。但控管者不得以保護他人權利為藉口拒絕正當近用主張，而是應採取技術措施滿足近用請求[81]。因此，當個資當事人就其數位足跡向控管者行使近用權時，控管者應考量對他人權利及自由之影響，並採取適當措施，在滿足當事人正當近用請求的同時，防範對他人權利及自由之不利影響。

其次，依 GDPR 第 11 條及第 12 條，控管者得在滿足近用權請求前驗證請求提出者係個資當事人，且若控管者無法識別個資當事人，則當事人之近用權將受到限制。GDPR 第 11 條規定，若控管者處理個人資料之目的不需或不再需要控管者識別個資當事人，則控管者應無義務為遵守 GDPR 之唯一目的，維持、取得或處理識別該個資當事人之額外資訊。此種情形下，若控管者能夠證明其無法識別當事人，則應在

[79] Article 29 Data Protection Working Party (WP29), Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (6 February 2018).
[80] EU, GDPR, §15(4), "The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others."
[81] EDPB, Guidelines 3/2019 on processing of personal data through video devices (10 July 2019), para. 94.

可行範圍內告知當事人。此時，不適用 GDPR 關於當事人近用權（第 15 條）及資料可攜權（第 20 條）之規範，但個資當事人為行使其權利而提供額外資訊，使其足以被辨識者，不在此限[82]。GDPR 前言第 57 點說明，若當事人為行使權利而提供額外資訊，控管者不得拒絕。相關額外資訊可能包括登入線上服務的驗證資訊等。依 GDPR 第 12 條第 6 項，控管者若對於近用權或資料可攜權請求之提出者是否係個資當事人存有疑問，得要求提供確認個資當事人身分之額外資訊[83]。

GDPR 前言第 64 點說明，在涉及線上服務及網路識別碼時，控管者尤其應採取一切合理措施驗證個資當事人身分。因此，個資當事人在就其數位足跡行使近用權時，應提供適當資訊表明其身分。若控管者無法透過其所處理的數位足跡識別個資當事人，則當事人僅在提供額外辨識性資訊之例外情形下，方可行使近用權。

第三，依 GDPR 第 12 條，控管者得限制或拒絕過度請求。依 GDPR 第 12 條第 5 項，若個資當事人提出過度或顯無理由之請求，特別是因重複提出請求而過度或顯無理由者，控管者得依行政成本收取合理費用，或拒絕對該請求採取行動。但控管者應證明該請求顯無理由或過度之性質[84]。

---

[82] EU, GDPR, §11, "1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation. 2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification."

[83] EU, GDPR, §12(6), "Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject."

[84] EU, GDPR, §12(5), "Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request."

此外，GDPR 前言第 63 點說明，若控管者處理有關當事人之大量資訊，得於傳遞資訊前，請求當事人具體說明所請求的資訊或處理作業。因此，若控管者有合理證據證明個資當事人就其數位足跡提出之近用權請求過度或顯無理由，得向當事人收取合理費用或拒絕該請求。

綜上所述，依歐盟 GDPR，數位足跡在可得識別自然人之前提下，係個人資料之一類，個資當事人得就其行使近用權，但應先表明其身分，或提供額外資訊驗證其身分。在不損害他人權利及自由、近用權請求非屬過度或顯無理由的前提下，控管者應提供數位足跡之副本。

（二）美國加州 CCPA

1、數位足跡是否構成個人資料

依美國加州 CCPA 第 1798.140 條第 v 項第 1 款定義[85]，個人資訊係指任何直接或間接辨識、關聯、描述或得合理連結至特定消費者或家庭的資訊，包括網路識別碼、IP 位址和獨特性個人識別碼（即可在相當一段時間內，跨越不同服務辨識特定消費者、家人或裝置的識別碼，例如裝置識別碼、IP 位址、cookie、beacon、pixel、手機廣告識別碼、使用者名稱等）（第 A 目），網際網路或其他電子網路活動資訊（如瀏覽歷史、搜尋歷史、消費者與特定網站應用程式或廣告的互

[85] California, CCPA (as amended by CPRA), §1798.140(v)(1), ""Personal information" means information that identifies, relates to, describes, is reasonably 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 if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household: (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…. (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 website application, or advertisement.… (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, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."

動等）（第 F 目），以及基於個人資訊所推知的、反映消費者偏好、特徵、心理傾向（psychological trend）、人格特質（predisposition）、行為、態度、智力、能力和天資（aptitude）的剖析檔案（第 K 目）。

同項第 2 款規定[86]，個人資訊不包括公開可得之資訊、合法取得的關於公共事務之真實資訊。所謂公開可得之資訊，包括：(1)可從聯邦、州或地方政府紀錄中合法取得之資訊；(2)業者合理相信係由該消費者或公開媒體合法提供予一般民眾之資訊；(3)該消費者揭露予某人且未限定資訊提供對象時，由該人提供之資訊。但業者在消費者不知情狀況下蒐集之生物特徵資料，不構成公開可得資料。

由此可知，在與特定消費者或家庭存在合理關聯的範圍內，美國加州 CCPA 已將消費者之數位足跡明文列舉為個人資訊之一類。但數位足跡中由消費者自行公開於網路之部分，例如公開之社群媒體貼文、購物網站上之公開評論等，並不屬於 CCPA 所規範的個人資訊。

2、CCPA 中的查閱權

CCPA 第 1798.110 條規定消費者知的權利和近用權。依該條第 a 項[87]，消費者有權請求業者（business）提供後者所蒐集其個人資訊之類別（第 1 款）和來源（第 2 款），蒐集、

[86] California, CCPA (as amended by CPRA), §1798.140(v)(2), ""Personal information" does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. For purposes of this paragraph, "publicly available" means: information that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media, or by the consumer; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge."

[87] California, CCPA (as amended by CPRA), §1798.110(a), "A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following: (1) The categories of personal information it has collected about that consumer. (2) The categories of sources from which the personal information is collected. (3) The business or commercial purpose for collecting, selling, or sharing personal information. (4) The categories of third parties to whom the business discloses personal information. (5) The specific pieces of personal information it has collected about that consumer."

銷售或分享其個人資訊之商業目的（第 3 款），個人資訊揭露對象之類別（第 4 款），以及所蒐集之特定個人資訊（specific pieces of personal information）（第 5 款）。

依同條第 b 項[88]，業者應在收到可驗證之消費者請求（verifiable consumer request）後，依該法規範提供所請求之資訊。且若該請求所涉個人資訊之類別和來源，蒐集、銷售或分享其個人資訊之商業目的，以及個人資訊揭露對象之類別，與業者線上隱私權通知中相關資訊完全相同，則視為業者已滿足同條第 a 項第 1 款至第 4 款規定之消費者資料權利。

依第 1798.130 條第 a 項第 3 款第 B 目之 iii 規定[89]，對於「自消費者取得」的特定個人資訊，應以一般消費者容易理解之格式提供，且在技術可行範圍內，應以結構化且機器可讀之通用格式提供，以便依消費者指示傳輸給另一主體。「特定個人資訊」不包括為確保安全或完整性而生成之資料。消費者亦得依第 1798.115 條，要求業者提供銷售與分享個人資訊之狀況。

對於落入個人資訊範圍之數位足跡，依前開規範，消費者得就其數位足跡，要求業者提供關於類別、來源、蒐集/銷售/分享目的、揭露對象類別方面之資訊。除數位足跡中由業

[88] California, CCPA (as amended by CPRA), §1798.110(b), "A business that collects personal information about a consumer shall disclose to the consumer, pursuant to subparagraph (B) of paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer, provided that a business shall be deemed to be in compliance with paragraphs (1) to (4), inclusive, of subdivision (a) to the extent that the categories of information and the business or commercial purpose for collecting, selling, or sharing personal information it would be required to disclose to the consumer pursuant to paragraphs (1) to (4), inclusive, of subdivision (a) is the same as the information it has disclosed pursuant to paragraphs (1) to (4), inclusive, of subdivision (c)."

[89] California, CCPA (as amended by CPRA), §1798.130(a)(3)(B), "For purposes of subdivision (b) of Section 1798.110:…(iii) Provide the specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance. "Specific pieces of information" do not include data generated to help ensure security and integrity or as prescribed by regulation. Personal information is not considered to have been disclosed by a business when a consumer instructs a business to transfer the consumer's personal information from one business to another in the context of switching services."

者為確保安全或完整性而自動生成的資料外，消費者亦得要求業者提供數位足跡之具體內容。數位足跡中由業者形成的剖析檔案，應不構成自消費者取得之特定個人資訊，因而不適用 CCPA 第 1798.130 條第 a 項第 3 款第 B 目之 iii 關於資訊提供格式之要求。但由業者自動記錄之數位足跡，是否構成「自消費者取得」的特定個人資訊並適用資訊提供格式要求，似有討論空間。

CCPA 第 1798.185 條第 a 項第 14 款授權州檢察長就「自消費者取得之資訊」之定義制定施行細則[90]。此一規範自 2020 年 12 月生效，但截至 2021 年 11 月，加州州檢察長尚未公布相關施行細則。加州隱私保護署 CPRA 細則公告中，包含「自消費者取得之資訊」之定義[91]。因此，加州消費者對其數位足跡行使查閱權之範圍，未來有望進一步明確。

3、 查閱權之行使限制

依 CCPA 及其施行細則[92]，當事人行使近用權時，可能受限制。首先，依 CCPA 第 1798.145 條第 k 項[93]，消費者依 CCPA 享有之權利不得對其他自然人之權利和自由有不利影響。若消費者之個人資訊屬於其他自然人所有，或係業者代表其他自然人維持（maintain），則消費者無法依同法第 1798.110 條請求提供該等個人資訊。因此，消費者就其數位足跡向業者行使知的權利時，業者應考量對其他自然人權利及自由之影響。

[90] California, CCPA (as amended by CPRA), §1798.185(a)(14).
[91] California Privacy Protection Agency, Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 (September 22, 2021), https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf.
[92] California Consumer Privacy Act Regulations.
[93] California, CCPA (as amended by CPRA), §1798.145(k), "(k) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other natural persons. A verifiable consumer request for specific pieces of personal information, pursuant to Section 1798.110 to delete a consumer's personal information, pursuant to Section 1798.105, or to correct inaccurate personal information, pursuant to Section 1798.106, shall not extend to personal information about the consumer that belongs to, or the business maintains on behalf of, another natural person. …"

此外，依 2020 年修正後的 CCPA 第 1798.185 條第 a 項第 3 款[94]，州檢察長應依據加州或聯邦層級的營業秘密、智慧財產保護及其他法律，就 CCPA 適用上的例外制定施行細則，以確保回應消費者權利行使請求時，不致揭露營業秘密。雖然截至 2021 年 11 月，加州州檢察長已頒行之施行細則中，尚未就營業秘密保護規定例外，但從 CCPA 該第 1798.185 條第 a 項第 3 款之規定可知，業者得於回應消費者知的權利請求時，考量營業秘密保護法律規範之要求。

其次，依 CCPA 第 1798.130 條第 a 項第 2 款，業者得合理要求提出請求之消費者驗證其身分（第 A 目）[95]。若提供所請求的資訊被證明為不可能或將勞費過鉅（disproportionate effort），則業者無需提供資訊（第 B 目）[96]。

且依 CCPA 施行細則第 999.313 條第 c 項第 3 款[97]，在同時具備下列條件時，業者無需搜尋所請求的個人資訊：(1)業者未以可搜尋或可合理存取的格式維持該個人資訊；(2)業者維持該個人資訊之唯一目的係法律或合規；(3)業者未銷售或為商業目的使用該個人資訊；(4)業者向消費者告知包含該個人資訊之紀錄類型。因此，消費者在就其數位足跡行使知的

[94] California, CCPA (as amended by CPRA), §1798.185(a), "On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas: … (3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter, with the intention that trade secrets should not be disclosed in response to a verifiable consumer request."

[95] California, CCPA (as amended by CPRA), §1798.130(a)(2)(A), "… The business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, …"

[96] California, CCPA (as amended by CPRA), §1798.130(a)(2)(B), "The disclosure of the required information shall cover the 12-month period preceding the business' receipt of the verifiable consumer request … and the business shall be required to provide that information unless doing so proves impossible or would involve a disproportionate effort. …"

[97] California CCPA Regulations § 999.313(c)(3), "In responding to a request to know, a business is not required to search for personal information if all of the following conditions are met: a. The business does not maintain the personal information in a searchable or reasonably accessible format; b. The business maintains the personal information solely for legal or compliance purposes; c. The business does not sell the personal information and does not use it for any commercial purpose; and d. The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above."

權利時，應驗證其身分，且業者得援用勞費過鉅等例外限制或拒絕提供個人資訊之具體內容。

第三，依 CCPA 第 1798.130 條第 a 項第 3 款[98]，消費者行使資料權利的對象以業者為限。業者的服務提供者（service provider）或承包商（contractor）就其以服務提供者或承包商身分蒐集的個資資訊，並無義務回應消費者提出之知的權利請求。依 CCPA 第 1798.140 條之定義，服務提供者係指代表業者處理個人資訊，且為商業目的自業者或代表業者接收個人資訊者，承包商係業者為商業目的而提供個人資訊之對象。業者應與服務提供者或承包商訂定書面契約，限制服務提供者/承包商的處理行為。因此，業者若利用第三方服務處理消費者個人資訊，消費者在就其數位足跡行使知的權利時，原則應向業者提出請求。

第四，依 CCPA 第 1798.145 條第 j 項第 1 款，對於通常業務活動中不會作為個人資訊加以維持之資訊，業者、服務提供者或承包商並無義務重新識別或以其他方式加以連結。依同項第 3 款，業者、服務提供者或承包商並無義務以可識別、可連結或可關聯之形式維持資訊，或蒐集、取得、保存或近用任何數據或技術，以便能夠將特定可驗證的消費者請求與個人資訊相連結或關聯[99]。因此，若業者所處理的數位足跡並不能夠識別特定消費者，業者並無義務透過取得額外資訊滿足消費者知的請求。

[98] California, CCPA (as amended by CPRA), §1798.130(a)(3), "…A service provider or contractor shall not be required to comply with a verifiable consumer request received directly from a consumer or a consumer's authorized agent, pursuant to Section 1798.110 or 1798.115, to the extent that the service provider or contractor has collected personal information about the consumer in its role as a service provider or contractor…."

[99] California, CCPA (as amended by CPRA), §1798.145(j), "(j) This title shall not be construed to require a business, service provider, or contractor to: (1) Reidentify or otherwise link information that, in the ordinary course of business, is not maintained in a manner that would be considered personal information….(3) Maintain information in identifiable, linkable, or associable form, or collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating a verifiable consumer request with personal information."

綜上所述，依美國加州 CCPA，非公開可得的數位足跡係該法明文規範之個人資訊，個資當事人得就其行使知的權利，但原則應直接向業者提出請求，並驗證其身分。若業者所處理的數位足跡無法識別特定消費者，業者得拒絕提出請求的消費者提供額外資訊以實現辨識。

（三）美國維吉尼亞州 CDPA

1、數位足跡是否構成個人資料

依 CDPA 第 59.1-571 條之定義[100]，「個人資料」係指與連結或可連結至某一已識別或可識別的自然人的任何資訊，但不包括已去識別化或公開可得之資訊。而所謂「公開可得之資訊」，係指可從聯邦、州或地方政府紀錄中合法取得之資訊，以及控管者合理相信係由下列人員合法提供予一般民眾之資訊：(1)該消費者，(2)公開媒體，(3)該消費者揭露該資訊之對象，但以該消費者未限定該資訊提供對象為限[101]。

據此，在與某一可識別的自然人相連結的範圍內，數位足跡構成個人資料。但數位足跡中由消費者自行公開於網路之部分，例如公開之社群媒體貼文，並不屬於 CDPA 所規範之個人資訊。

2、CDPA 中的查閱權

CDPA 第 59.1-573 條規定消費者享有之資料權利。該條第 A 項第 1 款規定[102]，消費者有權向控管者確認其是否處理個人

[100] Virginia, CDPA, §59.1-571, "…"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include de-identified data or publicly available information….".

[101] Virginia, CDPA, §59.1-571, "…"Publicly available information" means information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience…."

[102] Virginia, CDPA, §59.1-573(A), "A consumer may invoke the consumer rights authorized pursuant to this subsection at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to invoke. A known child's parent or legal guardian may invoke such consumer

資料，並存取該等個人資料。消費者得隨時提出權利行使請求，控管者應於驗證請求者身分後，滿足該請求。依 CDPA 第 59.1-574 條第 E 項規定[103]，控管者應建立一種或多種安全可靠的方法以供消費者提出行使權利之請求，並在隱私權聲明中說明相關方法。行使權利之方法應考量消費者與控管者互動的通常方式、提出請求時對安全可靠的通訊方式之需求，以及控管者驗證提出請求者身分的能力。

據此，對於落入個人資料範圍之數位足跡，消費者得向控管者確認數位足跡之處理狀況，並存取該等數位足跡。

3、 查閱權之行使限制

首先，依美國維吉尼亞州 CDPA 第 59.1-577 條第 C 項[104]，在同時具備下列條件時，控管者無須滿足已驗證之消費者權利請求：(1)控管者無法在合理範圍內將該請求連結至個人資料，或將該請求連結至個人資料將對控管者造成不合理之負擔；(2)控管者未將該個人資料用於識別或回覆作為資料主體之消費者，且未將該個人資料與同一消費者的其他個人資料相關聯；且(3)控管者未將該個人資料出售予第三人，亦未以其他方式將該個人資料自願揭露予處理者以外的其他第三人，但依該條規定得予以販售或以其他方式揭露者，不在此限。

rights on behalf of the child regarding processing personal data belonging to the known child. A controller shall comply with an authenticated consumer request to exercise the right: 1. To confirm whether or not a controller is processing the consumer's personal data and to access such personal data;…"

[103] Virginia, CDPA, §59.1-574(E), "A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights under this chapter. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to authenticate the identity of the consumer making the request. …"

[104] Virginia, CDPA, §59.1-577(C), "Nothing in this chapter shall be construed to require a controller or processor to comply with an authenticated consumer rights request, pursuant to § 59.1-573, if all of the following are true: 1. The controller is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data; 2. The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer; and 3. The controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section."

因此，若消費者就其數位足跡向控管者行使近用權，對於符合前述條件之數位足跡，控管者得拒絕提供。

第二，依CDPA第59.1-577條第D項[105]，對於假名資料，若控管者能夠證明用以辨識消費者的資訊被分開保存，且存在有效技術性及組織性管控措施防止控管者存取該等資訊，則不適用該法第 59.1-573 條第 A 項規定的近用權、更正權、刪除權和資料可攜權，以及第 59.1-574 條規定的控管者義務。因此，對於符合前述條件的假名化數位足跡，消費者不享有近用權，控管者無義務滿足消費者的近用權請求。

第三，依 CPDA 第 59.1-578 條第 E 項[106]，該法課予控管者或處理者之義務，不得對他人之權利或自由造成不利影響。據此，控管者回應消費者近用權請求時，應考量他人之權利與自由是否可能因此受到不利影響。

綜上所述，依美國維吉尼亞州 CDPA，非公開可得的數位足跡可能落入個人資料之範圍，個資當事人得就其行使近用權。但假名化數位足跡等，近用權可能有例外限制。

（四）日本個人資訊保護法

1、數位足跡是否構成個人資料

日本個人資訊保護法適用於「個人資訊處理事業」對個人資料之處理與保護。依該法第2條第5項[107]，「個人資訊處

[105] Virginia, CDPA, §59.1-577(D), "The consumer rights contained in subdivisions A 1 through 4 of § 59.1-573 and § 59.1-574 shall not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information."

[106] Virginia, CDPA, §59.1-578(E), "Nothing in this chapter shall be construed as an obligation imposed on controllers and processors that adversely affects the rights or freedoms of any persons, such as exercising the right of free speech pursuant to the First Amendment to the United States Constitution, or applies to the processing of personal data by a person in the course of a purely personal or household activity."

[107] 日本，個人情報の保護に関する法律（平成十五年法律第五十七号，令和二年法律第四十四号による改正，以下「個人情報保護法」という），§2(5)，「この法律において「個人情報取扱事業者」とは、個人情報データベース等を事業の用に供している者をいう。ただし、

理事業」係指國家機關、地方自治團體、獨立行政法人、地方獨立行政法人之外的其他事業。

依日本個人資訊保護法第2條第1項第1款規定[108]，因包含姓名、出生年月日以及其他記述而能識別存活中的特定個人之資訊，構成個人資訊。此處所稱「記述」，係指記載、記錄、或透過聲音、動作或其他方式表現之一切事項，並呈現為書面、畫面或電磁記錄者。而所謂「識別」，包括間接識別之情形，即透過「易於與其他資訊相結合比對而實現識別者」。

日本個人資訊保護法另包含「個人資料」之定義，即構成個人資訊資料庫之個人資訊[109]。而「個人資訊資料庫」係指符合下列條件之個人資訊之集合物：(1)經系統化整理，因而得利用電腦檢索特定個人資訊者；(2)政令規範的其他經系統化整理而易於檢索特定個人資訊者[110]。而個人資訊處理事

次に掲げる者を除く。一　国の機関。二　地方公共団体。三　独立行政法人等（独立行政法人等の保有する個人情報の保護に関する法律（平成十五年法律第五十九号）第二条第一項に規定する独立行政法人等をいう。以下同じ。）。四　地方独立行政法人（地方独立行政法人法（平成十五年法律第百十八号）第二条第一項に規定する地方独立行政法人をいう。以下同じ。）」。

[108] 日本，個人情報保護法，§2(1)(1)，「この法律において「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。一　当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第二号において同じ。）で作られる記録をいう。第十八条第二項及び第二十八条第一項において同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」。

[109] 日本，個人情報保護法，§2(6)，「この法律において「個人データ」とは、個人情報データベース等を構成する個人情報をいう。」。

[110] 日本，個人情報保護法，§2(4)，「この法律において「個人情報データベース等」とは、個人情報を含む情報の集合物であって、次に掲げるもの（利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定めるものを除く。）をいう。一　特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの。二　前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの。」。

業有權揭露、更正、補充或刪減內容、停止利用、刪除、停止對第三人提供之個人資料，為「保有個人資料」[111]。

日本個人資訊保護法於 2020 年修正時，於第 26-2 條增設「個人關聯資訊」之概念（即與生存之人相關，但不構成個人資訊、假名個人資訊或匿名個人資訊之資訊）[112]，並就個人關連資訊向第三人之揭露增設限制。

據此，可直接或間接識別特定個人之數位足跡，應構成個人資訊；其中已納入個人資訊資料庫者，為個人資料；個人資訊處理事業有權處理之個人資料，即為「保有個人資料」。而若數位足跡無從直接或間接識別特定個人，因其係生存之人活動所產生，應屬「個人關連資訊」。

2、日本個資法中的查閱權

依日本個人資訊保護法第 28 條第 1 項[113]，個資當事人得請求個人資訊處理事業，以提供電磁紀錄或個人資訊保護委員會規則規定的其他方式，揭露能識別該當事人之保有個人資料。依同條第 2 項[114]，個人資訊處理事業於收到請求後，原則應儘速揭露所請求之個人資料。2020 年修正時，日本個人資訊保護法並調整個人資訊處理事業對當事人查閱請求之回應方式，由「得以電子或書面方式提供」改為「得以依當

[111] 日本，個人情報保護法，§2(7)，「この法律において「保有個人データ」とは、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの以外のものをいう。」。

[112] 日本，個人情報保護法，§26-2，「個人関連情報取扱事業者（個人関連情報データベース等（個人関連情報（生存する個人に関する情報であって、個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないものをいう。以下同じ。）…」。

[113] 日本，個人情報保護法，§28(1)，「本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データの電磁的記録の提供による方法その他の個人情報保護委員会規則で定める方法による開示を請求することができる。」。

[114] 日本，個人情報保護法，§28(2)，「個人情報取扱事業者は、前項の規定による請求を受けたときは、本人に対し、同項の規定により当該本人が請求した方法（当該方法による開示に多額の費用を要する場合その他の当該方法による開示が困難である場合にあっては、書面の交付による方法）により、遅滞なく、当該保有個人データを開示しなければならない。」。

事人指示方式提供」。另依日本個人資訊保護法第 32 條第 1 項及個人資訊保護法施行令第 10 條，個人資訊處理事業得訂立個資當事人請求之受理對象、請求之格式、個資當事人代理人身分之確定方式、收費方法等。依同法第 32 條第 4 項[115]，個人資訊處理事業對個資當事人請求之回覆程序，不得對個資當事人造成過重負擔。

據此，對於構成個人資料之數位足跡，個資當事人得請求個人資訊處理事業予以揭露。

3、 查閱權之行使限制

首先，依日本個人資訊保護法第 28 條第 2 項[116]，存在下列情形之一時，個人資訊處理事業得拒絕揭露所請求個人資料之全部或一部：(1)揭露可能損害個資當事人或第三人的生命、身體、財產或其他利益；(2)揭露可能嚴重損害個人資訊處理事業之正常經營；(3)揭露將違反其他法令。據此，個人資訊處理事業得援用前開理由，特別是對正常經營活動之嚴重損害，拒絕滿足個資當事人之揭露請求。

其次，依日本個人資訊保護法第 32 條第 2 項[117]，個人資訊處理事業得要求個資當事人具體說明請求揭露之具體對象。

---

[115] 日本，個人情報保護法，§32(4)，「個人情報取扱事業者は、前三項の規定に基づき開示等の請求等に応じる手続を定めるに当たっては、本人に過重な負担を課するものとならないよう配慮しなければならない。」。

[116] 日本，個人情報保護法，§28(2)，「個人情報取扱事業者は、前項の規定による請求を受けたときは、本人に対し、同項の規定により当該本人が請求した方法（当該方法による開示に多額の費用を要する場合その他の当該方法による開示が困難である場合にあっては、書面の交付による方法）により、遅滞なく、当該保有個人データを開示しなければならない。ただし、開示することにより次の各号のいずれかに該当する場合は、その全部又は一部を開示しないことができる。一　本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合。二　当該個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合。三　他の法令に違反することとなる場合」。

[117] 日本，個人情報保護法，§32(2)，「個人情報取扱事業者は、本人に対し、開示等の請求等に関し、その対象となる保有個人データ又は第三者提供記録を特定するに足りる事項の提示を求めることができる。この場合において、個人情報取扱事業者は、本人が容易かつ的確に開示等の請求等をすることができるよう、当該保有個人データ又は当該第三者提供記録の特定に資する情報の提供その他本人の利便を考慮した適切な措置をとらなければならない。」。

依同法第 33 條[118]，個人資訊處理事業得就個資當事人之揭露請求，向當事人酌收合理費用，費用金額應與實際成本相當。據此，個資當事人之揭露請求應有相當具體性，且當事人應負擔揭露之成本。

第三，依日本個人資訊保護法第 35-2 條第 9 項[119]，假名資訊、構成假名資料之個人資料以及構成假名資料之保有個人資料，不適用第 28 條所規定之請求揭露之權利。據此，對於已經假名化處理之個人資料，個人資訊處理事業得拒絕個資當事人之揭露請求。

綜上所述，依日本個人資訊保護法，對於具有直接或間接識別性，且已納入個人資訊數據庫之數位足跡，個資當事人得向個人資訊處理事業請求揭露。但在嚴重損害個人資訊處理事業正常經營等情形下，業者得全部或部分拒絕揭露請求。於該法配合數位社會整備法修正後，前開規範雖有條號及文字調整，但其內容並無實質變化。

（五）日本行政機關個人資訊保護法

1、數位足跡是否構成個人資料

日本行政機關個人資訊保護法關於個人資訊之定義與個人資訊保護法相似。依行政機關個人資訊保護法第 2 條第 2 項第 1 款規定[120]，因包含姓名、出生年月日以及其他記述而能

[118] 日本，個人情報保護法，§33，「１　個人情報取扱事業者は、第二十七条第二項の規定による利用目的の通知を求められたとき又は第二十八条第一項の規定による開示の請求を受けたときは、当該措置の実施に関し、手数料を徴収することができる。２　個人情報取扱事業者は、前項の規定により手数料を徴収する場合は、実費を勘案して合理的であると認められる範囲内において、その手数料の額を定めなければならない。」。

[119] 日本，個人情報保護法，§35-2(9)，「仮名加工情報、仮名加工情報である個人データ及び仮名加工情報である保有個人データについては、第十五条第二項、第二十二条の二及び第二十七条から第三十四条までの規定は、適用しない。」。

[120] 日本，行政機関の保有する個人情報の保護に関する法律（平成十五年法律第五十八号，令和元年法律第三十七号による改正，以下「行政機關個人情報保護法」という），§2(2)(1)，「この法律において「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。一　当該情報に含まれる氏名、生年月日その他の記述等

識別存活中的特定個人之資訊，構成個人資訊。此處所稱「記述」，係指記載、記錄、或透過聲音、動作或其他方式表現之一切事項，並呈現為書面、畫面或電磁紀錄者。而所謂「識別」，包括間接識別之情形，即透過「與其他資訊相結合比對而實現識別者」。行政機關個人資訊保護法並未定義「個人資料」。

「保有個人資訊」係指行政機關職員在執行職務過程中做成或取得、由該機關保有以供其職員組織性利用之個人資訊，但以記載於「行政文書」中者為限[121]。所謂「行政文書」，依日本行政機關資訊公開法之定義，係指行政機關職員在執行職務過程中做成或取得、由該機關保有以供其職員組織性利用之書面、畫面或電磁紀錄，但不包括政府公報、白皮書、報紙、雜誌、書籍等對於不特定多數人以販售為目的所發行者；或在政令所定之國立公文書館（即日本國家檔案館）或其他機關，作為歷史或文化的、學術研究的資料之用而受特別之管理者[122]。

（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第二号において同じ。）で作られる記録をいう。以下同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）により特定の個人を識別することができるもの（他の情報と照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」。

121 日本，行政機關個人情報保護法，§2(5)，「この法律において「保有個人情報」とは、行政機関の職員が職務上作成し、又は取得した個人情報であって、当該行政機関の職員が組織的に利用するものとして、当該行政機関が保有しているものをいう。ただし、行政文書（行政機関の保有する情報の公開に関する法律（平成十一年法律第四十二号。以下「行政機関情報公開法」という。）第二条第二項に規定する行政文書をいう。以下同じ。）に記録されているものに限る。」。

122 日本，行政機関の保有する情報の公開に関する法律，§2(5)，「この法律において「行政文書」とは、行政機関の職員が職務上作成し、又は取得した文書、図画及び電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。以下同じ。）であって、当該行政機関の職員が組織的に用いるものとして、当該行政機関が保有しているものをいう。ただし、次に掲げるものを除く。一　官報、白書、新聞、雑誌、書籍その他不特定多数の者に販売することを目的として発行されるもの。二　公文書等の管理に関する法律（平成二十一年法律第六十六号）第二条第七項に規定する特定歴史公文書等。三　政令で定める研究所その他の施設において、政令で定めるところにより、歴史的若しくは文化的な資料又は学術研究用の資料として特別の管理がされているもの（前号に掲げるものを除く。）」。

據此，行政機關在執行公務過程中作成或取得並留作公務運用，記載於行政文書之中，可直接或間接識別個資當事人之數位足跡，應構成保有個人資訊。

2、日本行政機關個人資訊保護法中的查閱權

依日本行政機關個人資訊保護法第 12 條第 1 項[123]，就行政機關所保有之個人資訊，個資當事人得向該行政機關之首長請求揭露。揭露請求應依同法第 13 條提交揭露請求書。日本行政機關個人資訊保護法第 14 條規定[124]，除有法定例外情形外，收到請求之行政機關應向作出請求之個資當事人揭露所請求的保有個人資訊。依同法第 15 條[125]，若被請求之保有個人資訊之一部存在法定不得揭露之情形，行政機關應在可行情形下，除去不得揭露之部分後，將剩餘部分揭露予作出請求之個資當事人。

依同法第 16 條[126]，對於存在法定不得揭露情形之個人資料，行政機關首長得基於個人權益保護之特別需求，裁量予以揭露。因此，對於屬於保有個人資訊之數位足跡，個資當事人得請求行政機關予以揭露。

[123] 日本，行政機關個人情報保護法，§12(1)，「何人も、この法律の定めるところにより、行政機関の長に対し、当該行政機関の保有する自己を本人とする保有個人情報の開示を請求することができる。」。

[124] 日本，行政機關個人情報保護法，§14，「行政機関の長は、開示請求があったときは、開示請求に係る保有個人情報に次の各号に掲げる情報（以下「不開示情報」という。）」。

[125] 日本，行政機關個人情報保護法，§15(1)，「行政機関の長は、開示請求に係る保有個人情報に不開示情報が含まれている場合において、不開示情報に該当する部分を容易に区分して除くことができるときは、開示請求者に対し、当該部分を除いた部分につき開示しなければならない。」。

[126] 日本，行政機關個人情報保護法，§16，「行政機関の長は、開示請求に係る保有個人情報に不開示情報が含まれている場合であっても、個人の権利利益を保護するため特に必要があると認めるときは、開示請求者に対し、当該保有個人情報を開示することができる。」。

3、 查閱權之行使限制

依日本行政機關個人資訊保護法第 14 條[127]，於下列情形，行政機關得拒絕揭露所請求之保有個人資訊：(1)該資訊對提出請求之個資當事人生命、健康、生計、財產有侵害之虞；(2)除法律另有規定、保護個人權益、公職人員執行職務紀錄等例外情形外，該資訊可識別個資當事人以外其他人之個人資訊，或揭露該資訊對他人之權益有侵害之虞；(3)該資訊可能影響其他企業之權利、競爭地位或正當利益，或該資訊係其他企業依合理保密條件自願提供予行政機關之資訊；(4)該行政機關首長合理認為揭露該資訊可能妨礙國家安全或國際關係；(5)該行政機關首長合理認為揭露該資訊可能妨礙犯罪預防、刑事追訴或公共安全；(7)該資訊涉及行政機關內部或

[127] 日本，行政機關個人情報保護法，§14，「行政機関の長は、開示請求があったときは、開示請求に係る保有個人情報に次の各号に掲げる情報（以下「不開示情報」という。）のいずれかが含まれている場合を除き、開示請求者に対し、当該保有個人情報を開示しなければならない。一　開示請求者（第十二条第二項の規定により未成年者又は成年被後見人の法定代理人が本人に代わって開示請求をする場合にあっては、当該本人をいう。次号及び第三号、次条第二項並びに第二十三条第一項において同じ。）の生命、健康、生活又は財産を害するおそれがある情報。二　開示請求者以外の個人に関する情報（事業を営む個人の当該事業に関する情報を除く。）であって、当該情報に含まれる氏名、生年月日その他の記述等により開示請求者以外の特定の個人を識別することができるもの（他の情報と照合することにより、開示請求者以外の特定の個人を識別することができることとなるものを含む。）若しくは個人識別符号が含まれるもの又は開示請求者以外の特定の個人を識別することはできないが、開示することにより、なお開示請求者以外の個人の権利利益を害するおそれがあるもの。……三　法人その他の団体（国、独立行政法人等、地方公共団体及び地方独立行政法人を除く。以下この号において「法人等」という。）に関する情報又は開示請求者以外の事業を営む個人の当該事業に関する情報であって、次に掲げるもの。ただし、人の生命、健康、生活又は財産を保護するため、開示することが必要であると認められる情報を除く。……四　開示することにより、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあると行政機関の長が認めることにつき相当の理由がある情報。五　開示することにより、犯罪の予防、鎮圧又は捜査、公訴の維持、刑の執行その他の公共の安全と秩序の維持に支障を及ぼすおそれがあると行政機関の長が認めることにつき相当の理由がある情報。六　国の機関、独立行政法人等、地方公共団体及び地方独立行政法人の内部又は相互間における審議、検討又は協議に関する情報であって、開示することにより、率直な意見の交換若しくは意思決定の中立性が不当に損なわれるおそれ、不当に国民の間に混乱を生じさせるおそれ又は特定の者に不当に利益を与え若しくは不利益を及ぼすおそれがあるもの。七　国の機関、独立行政法人等、地方公共団体又は地方独立行政法人が行う事務又は事業に関する情報であって、開示することにより、次に掲げるおそれその他当該事務又は事業の性質上、当該事務又は事業の適正な遂行に支障を及ぼすおそれがあるもの。……」。

相互間之議事過程，且揭露該資訊將影響正常議事或造成特定人之利益或不利益；(8)該資訊涉及行政機關之業務，且揭露該資訊可能妨礙正常辦理該等業務。據此，個資當事人請求行政機關揭露其數位足跡時，可能面臨諸多限制。

綜上所述，依日本行政機關個人資訊保護法，對於具有直接或間接識別性，由行政機關在執行公務過程中作成或取得並留作公務運用，記載於行政文書之中之數位足跡，個資當事人得向行政機關請求揭露。但行政機關得援用該法規定之限制條件，拒絕揭露所請求資訊之全部或一部。該法配合數位社會整備法修正，併入個人資訊保護法後，前開規範雖有條號及文字調整，但其內容並無實質變化。

（六）韓國個人資料保護法

1、數位足跡是否構成個人資料

依韓國個人資料保護法第2條第1項之定義[128]，個人資料係指藉由姓名、身分證號碼、影像等而得以識別特定個人之資訊，以及自身雖不具識別性，但可輕易與其他資訊結合而識別特定個人之資訊。「輕易結合」之判定，需考量實現辨識所需時間、費用、技術，以及取得所結合資訊之可能性等。假名資料（即經假名化處理之資料）亦屬於個人資料。

因此，可直接識別個資當事人之數位足跡構成個人資料應無疑問。自身不具辨識性之數位足跡是否構成個人資料，尚需就其與其他資料結合以實現辨識之難易程度進行個案判

[128] 한국，개인정보보호법，§2(1)，“‘개인정보”란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다. 가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보. 나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.”

斷，但可以推斷，若業者累積同一使用者的大量數位足跡，則透過結合其他資訊識別該使用者之可能性將會相應提高。

2、韓國個資法中的查閱權

依韓國個人資料保護法第 4 條第 3 項[129]，個資當事人得向個人資料處理者確認其個人資料是否被處理，並請求閱覽（包含提供複本）。

同法第 35 條係關於個資當事人閱覽權之細部規範[130]。依據該條第 1 項，個資當事人得向個人資料處理者要求閱覽其被後者處理之個人資料。依同條第 2 項，若個資當事人行使閱覽權之對象係一公共機構，則除直接向該機構提出請求外，亦可依大統領規定向個人資料保護委員會提出請求。

依個人資料保護法第 38 條第 4 項[131]，個人資料處理者應訂定行使個資當事人權利之詳盡方法和程序，並公告該等方法和程序以利個資當事人知悉。依同條第 5 項，個人資料處理者應訂定並提供相應程序，以利請求被拒絕的個資當事人提出異議。

由以上可知，對於屬於個人資料之數位足跡，個資當事人有權向個人資料處理者請求閱覽。

---

[129] 한국，개인정보보호법，§4，“정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진 다. … 3. 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람(사본의 발급을 포함한다. 이하 같다)을 요구할 권리.”

[130] 한국 ，개인정보보호법 ，§35 ，“① 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다. ② 제 1 항에도 불구하고 정보주체가 자신의 개인정보에 대한 열람을 공공기관에 요구하고자 할 때에는 공공기관에 직접 열람을 요구하거나 대통령령으로 정하는 바에 따라 보호위원회를 통하여 열람을 요구할 수 있다.”

[131] 한국，개인정보보호법，§38，“…④ 개인정보처리자는 정보주체가 열람등요구를 할 수 있는 구체적인 방법 과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다. ⑤ 개인정보처리자는 정보주체가 열람등요구에 대한 거절 등 조치에 대하 여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.”

3、 查閱權之行使限制

首先，依韓國個人資料保護法第 35 條第 4 項[132]，有下列情形之一時，個人資料處理者得限制或拒絕個資當事人之閱覽請求：(1)依法律禁止或限制閱覽；(2)閱覽有危害他人生命或身體之虞，或有不當侵害他人之財產或其他利益之虞；(3)公務機關執行稅捐、教育、考評、補償及福利決策、稽核與查檢等職務時遇有嚴重困難。依個人資料保護法施行令第 42 條[133]，若個人資料處理者依前開規範限制閱覽，仍應向個資當事人提供無前開情形之部分，若拒絕閱覽，應向個資當事人告知理由。

其次，依韓國個人資料保護法第 38 條第 3 項規定[134]，個人資料處理者得向當事人收取閱覽費，若當事人請求郵寄個人資料副本時，亦得收取郵資。依個人資料保護法施行令第

---

132 한국，개인정보보호법，§35(4)，“개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주 체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다. 1. 법률에 따라 열람이 금지되거나 제한되는 경우. 2. 다른 사람의 생명・신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우. 3. 공공기관이 다음 각 목의 어느 하나에 해당하는 업무를 수행할 때 중대한 지장을 초래하는 경우. 가. 조세의 부과・징수 또는 환급에 관한 업무. 나. 「초・중등교육법」 및 「고등교육법」에 따른 각급 학교, 「평생교육법」에 따른 평생교육시설, 그 밖의 다른 법률에 따라 설치된 고등교육기관에서의 성적 평가 또는 입학자 선발에 관한 업무. 다. 학력・기능 및 채용에 관한 시험, 자격 심사에 관한 업무. 라. 보상금・급부금 산정 등에 대하여 진행 중인 평가 또는 판단에 관한 업무. 마. 다른 법률에 따라 진행 중인 감사 및 조사에 관한 업무.”

133 한국，개인정보보호법시행령，§42，“① 개인정보처리자는 제 41 조제 1 항에 따른 열람 요구 사항 중 일부가 법 제 35 조제 4 항 각 호의 어느 하나에 해당하는 경우에는 그 일부에 대하여 열람을 제한할 수 있으며, 열람이 제한되는 사항을 제외한 부분은 열람할 수 있도록 하여야 한다.② 개인정보처리자가 법 제 35 조제 3 항 후단에 따라 정보주체의 열람을 연기하거나 같은 조 제 4 항에 따라 열람을 거절하려는 경우에는 열람 요구를 받은 날부터 10 일 이내에 연기 또는 거절의 사유 및 이의제기방법을 보호위원회가 정하여 고시하는 열람의 연기・거절 통지서로 해당 정보주체에게 알려야 한다.”

134 한국 ， 개인정보보호법 ， § 38(3) ， “개인정보처리자는 열람등요구를 하는 자에게 대통령령으로 정하는 바에 따라 수수료와 우송료(사본의 우송을 청구하는 경우에 한한다)를 청구 할 수 있다.”

47 條[135]，閱覽費及郵資之金額應以實際成本為限，且若個資當事人請求閱覽係因由個人資料處理者引起，個人資料處理者不得收取費用。

第三，依韓國個人資料保護法第 28-7 條[136]，同法第 35 條之規定不適用於假名資訊。因此，若個人資料處理者已對數位足跡進行假名化處理，個資當事人則不得對該等數位足跡行使閱覽權。

綜上所述，依韓國個人資料保護法，對於具有直接或間接識別性之數位足跡，個資當事人得向個人資料處理者請求閱覽，個人資料處理者得援引法定例外情形拒絕或限制閱覽。但若控管者已對數位足跡進行假名化處理，則個資當事人即無權請求閱覽該等數位足跡。

（七）新加坡個人資料保護法

1、數位足跡是否構成個人資料

依新加坡 PDPA 第 2 條之定義，個人資料係指與特定個人相關，符合下列條件之一，且不問其真實與否之資料：(1)可識別該特定個人，或(2)與該組織持有或可能存取之其他資訊結合後，可識別該特定個人[137]。

---

[135] 한국，개인정보보호법시행령，§47，“① 법 제 38 조제 3 항에 따른 수수료와 우송료의 금액은 열람등요구에 필요한 실비의 범위에서 해당 개인정보처리자가 정하는 바에 따른다. 다만, 개인정보처리자가 지방자치단체인 경우에는 그 지방자치단체의 조례로 정하는 바에 따른다. ② 개인정보처리자는 열람등요구를 하게 된 사유가 그 개인정보처리자에게 있는 경우에는 수수료와 우송료를 청구해서는 아니 된다. …”

[136] 한국，개인정보보호법，§28-7，“가명정보는 제 20 조, 제 21 조, 제 27 조, 제 34 조제 1 항, 제 35 조부터 제 37 조까지, 제 39 조의 3, 제 39 조의 4, 제 39 조의 6 부터 제 39 조의 8 까지의 규정을 적용하지 아니한다.”

[137] Singapore, PDPA, §2(1), “…“personal data” means data, whether true or not, about an individual who can be identified —(a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access;…”

新加坡 PDPA 另將「使用者活動資料」定義為個人在使用組織提供之產品或服務過程中生成、或因其使用所生成之個人資料；將「使用者提供資料」定義為個人向組織提供之個人資料[138]，並包含關於此兩類資料之特別規範。

據此，可直接辨識特定個人之數位足跡，應構成個人資料。但對於間接辨識性之數位足跡，若組織未持有或無法存取協助實現辨識的其他資訊，則該等數位足跡不屬於個人資料。屬於個人資料之數位足跡中，因該個人使用組織提供之網路產品或服務而生成之部分，將構成使用者活動資料；該個人提供之部分，將構成「使用者提供資料」。

2、新加坡個資法中的查閱權

PDPA 第 21 條係關於近用權之規範[139]。依該條，個人得向組織提出請求，要求該組織提供所持有或控制的關於該個人之個人資料，以及關於該個人資料最近一年內的利用與分享狀況之資訊。非有法定例外情形，組織應儘速提供所請求之資料及相關資訊。若所請求的個人資料與資訊中，適用法定例外情形之部分可與其他部分相分離，則組織應向提出請求者提供不適用法定例外之個人資料與資訊。

據此，若個資當事人就構成個人資料之數位足跡行使近用權，組織原則應滿足其近用請求。

[138] Singapore, PDPA, §2(1), "… "user activity data", in relation to an organisation, means personal data about an individual that is created in the course or as a result of the individual's use of any product or service provided by the organisation; "user-provided data", in relation to an organisation, means personal data provided by an individual to the organisation…."

[139] Singapore, PDPA, §21, "(1) Subject to subsections (2), (3) and (4), on request of an individual, an organisation shall, as soon as reasonably possible, provide the individual with —(a) personal data about the individual that is in the possession or under the control of the organisation; and (b) information about the ways in which the personal data referred to in paragraph (a) has been or may have been used or disclosed by the organisation within a year before the date of the request.… (5) If an organisation is able to provide the individual with the individual's personal data and other information requested under subsection (1) without the personal data or other information excluded under subsections (2), (3) and (4), the organisation shall provide the individual with access to the personal data and other information without the personal data or other information excluded under subsections (2), (3) and (4)."

3、查閱權之行使限制

依新加坡 PDPA 第 21 條第 2 項，有該法附表 5 所列情事時，組織「得拒絕」提供所請求之個人資料和資訊。

依附表 5 第 1 項第 g 款[140]，若提供該個人資料將造成機密商業資訊之揭露，且依合理之人（a reasonable person）判斷，將損害該組織的競爭地位，則組織無需遵守所收到的請求。依同項第 j 款[141]，組織可拒絕滿足下列該請求：(1)由於其重複性或系統性，將不當影響組織之運作，判定重複性或系統性時，得考慮組織收到請求之數量及頻率；(2)提供近用之負擔或成本對於該組織而言並不合理，或與該個人之利益不成比例；(3)所請求之資訊並不存在或無法找到；(4)所請求之資訊並無實質重要性；(6)其他瑣碎（frivolous）或無理（vexatious）的請求。若當事人之近用權請求可能不當損害組織之競爭力、對組織造成過重負擔，或該請求並無實質重要性，組織得拒絕滿足該請求。

依新加坡 PDPA 第 21 條第 3 項[142]，若合理認為存在下列情事，組織「不得」提供所請求之個人資料和（或）資訊：(1)提供該資料和（或）資訊將威脅提出請求者以外其他人的

[140] Singapore, PDPA 5th Schedule, §1, "An organisation is not required to provide information under section 21(1) in respect of —… (g) personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation;…"

[141] Singapore, PDPA 5th Schedule, §1, "An organisation is not required to provide information under section 21(1) in respect of —… (j) any request — (i) that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests; (ii) if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests; (iii) for information that does not exist or cannot be found; (iv) for information that is trivial; or (v) that is otherwise frivolous or vexatious."

[142] Singapore, PDPA, §21, "(3) Subject to subsection (3A), an organisation shall not provide an individual with the individual's personal data or other information under subsection (1) if the provision of that personal data or other information, as the case may be, could reasonably be expected to —(a) threaten the safety or physical or mental health of an individual other than the individual who made the request; (b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request; (c) reveal personal data about another individual; (d) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity; or (e) be contrary to the national interest. (3A) Subsection (3)(c) and (d) does not apply to any user activity data about, or any user-provided data from, the individual who made the request despite such data containing personal data about another individual."

安全或身心健康；(2)提供該資料和（或）資訊將對提出請求者安全或身心健康造成急迫或嚴重損害；(3)提供該資料和（或）資訊將揭露其他人之個人資料；(4)個人資料係由其他自然人提供，且該其他自然人未同意揭露其身分，提供該資料和（或）資訊將揭露該其他自然人之身分；(5)提供該資料和（或）資訊將違反國家利益。但提出請求者相關之「使用者活動資料」，以及提出請求者提供之「使用者提供資料」，縱包含其他人之個人資料，亦不適用前開第(3)和第(4)之例外。由前觀之，若當事人對於構成個人資料的數位足跡行使近用權，法定不得揭露情事之適用範圍相對限縮。

綜上所述，依新加坡 PDPA，對於具有直接或間接識別性之數位足跡，個人得向組織請求近用，組織得援引法定例外情形拒絕近用。但若數位足跡構成「使用者活動資料」或「使用者提供資料」，則法定例外之適用將相對限縮。

四、法規比較

自上述比較法觀察，當事人之查閱權（近用權）係各國個資法規通行之權利，惟權利之行使範圍與限制有不同規範。關於當事人可否就其數位足跡行使個資法上的查閱權，以下將從三個層面分別比較。

（一）數位足跡是否構成個人資料

依本報告比較研究之我國及其他各國個資法律，數位足跡在具有直接或間接識別性之前提下，原則上應屬個人資料。

其中，美國加州 CCPA 將消費者之「網際網路或其他電子網路活動資訊」明文列舉為個人資料，並以瀏覽歷史、搜尋歷史、與特定網站應用程式或廣告的互動等作為網路活動資訊之示例。此外，消費者網路活動所生成或使用之識別碼，

例如IP位址、cookie、beacon、pixel、手機廣告識別碼等，則被列為個人資料中「識別碼」之示例。歐盟 GDPR 對個人資料之定義示例雖未納入「網路活動或行為之紀錄」，但包含與網路活動密切相關之「網路識別碼」。

我國、美國維吉尼亞州、日本、韓國和新加坡的個資法律對「個人資料」之定義，皆未明文提及數位足跡，因此需對個案所涉數位足跡是否具有直接或間接識別性作具體判斷。能夠直接或間接識別特定當事人之數位足跡，原則構成個人資料，但可能有如下例外：

1、 間接識別性之限制

我國與歐盟 GDPR 關於「個人資料」之定義雖細部不同，但整體內涵一致，且其共通點之一係，並不要求所有足使特定當事人被識別之資料都必須由同一人掌握[143]。由美國維吉尼亞州 CDPA 之文句觀察，其所定義之個人資料包含可間接連結至特定個人之資訊，且未明文要求控管者掌握實現間接識別所需之其他資訊。由此可推知，CDPA 關於間接識別之要求，類似我國個資法和歐盟 GDPR。考量利用數位足跡追蹤使用者已是網路世界之現實狀況，應可認依我國、歐盟、美國維吉尼亞州個資法律，數位足跡原則具有間接識別性。

相較之下，日本、韓國和新加坡之個資法律對「間接識別性」有明文限制。日本與韓國皆將間接識別限定為「『易於』與其他資訊相結合比對」者。而新加坡則將間接識別定義為「與該組織『持有或可能存取』之其他資訊結合」而實現識別。據此，依日本、韓國和新加坡法規，數位足跡是否具有間接識別性，需依個案判斷。

[143] 見國家發展委員會 109 年 7 月 24 日發法字第 1090015912 號函；Court of Justice of the European Union (CJEU), Patrick Breyer v Bundesrepublik Deutschland (Case C‑582/14), Judgment of 19 October 2016, para. 43.

2、公開可得資料之限制

我國、歐盟、日本、韓國和新加坡的個資法律並未將「公開可得」（含依法公開）之資訊排除於個人資料之定義外，而是就公開可得之個人資料之蒐集、處理、利用訂有特別規範。據此，公開可得之數位足跡（如當事人之網路貼文等），仍屬個人資料，惟其蒐集處理利用規則可能與非公開可得之資料不同。相較之下，美國加州 CCPA 與維吉尼亞州 CDPA 將公開可得之資訊明文排除於個人資料之定義外。這意味著，公開可得之數位足跡直接排除於個人資料範圍外，當事人無法就公開可得之數位足跡行使資料權利。

（二）個資法中的查閱權

由前述各國法律規範觀察，對於構成個人資料之數位足跡，當事人原則可行使查閱權，但查閱權之範圍、行使方式等不盡一致，就其中與數位足跡關係緊密者分析如下：

1、查閱權之內涵

首先係查閱權之內涵，依我國個資法，查詢、閱覽個人資料與請求製給個人資料複製本，分屬不同權利。且依主管機關之見解，於當事人請求「閱覽」之情形，不得以「製給複製本」代替[144]。據此可認，我國個資法上的閱覽權，側重於當事人請求閱覽蒐集機關保留之個人資料「原件」之權利。

韓國個人資料保護法所規定之「閱覽權」包含要求提供複製本之權利，但閱覽與提供複製本可否互相替代，未見明文規範。相較之下，其他各國之個資法律，未見對於「閱覽原件」之特別保障。其中，歐盟、美國加州、美國維吉尼亞州和新加坡個資法律所保障之當事人查閱權，內容包括當事

[144] 見法務部 102 年 3 月 12 日法律字第 10100271950 號函。

人要求蒐集機關提供個資蒐集、利用、揭露等方面之資訊，並取得複製本。日本個資法律則係以「揭露」個人資料作為滿足當事人查閱權之方式。

數位足跡往往係蒐集機關自動記錄，針對特定當事人未必有系統性檔案，因此，就數位足跡之查閱權，我國個資法宜將查詢、閱覽與請求製給複製本三類權能作整體考量。

2、當事人可否就基於數位足跡做成的剖析檔案、自動化決策等，行使查閱權

前述各國個資法律中，歐盟 GDPR 明文將剖析和自動化決策列入近用權之行使範圍，個資當事人得據以取得剖析檔案之輸入資料，並得瞭解控管者將其資料用於自動化決策之相關資訊。美國加州 CCPA 則將「基於個人資訊所推知的、反映消費者偏好、特徵、心理傾向、人格特質、行為、態度、智力、能力和天資的剖析檔案」明定為個人資訊之一類。至於其他各國之個資法律，皆未就剖析檔案、自動化決策等予以明文納入或排除。有利於個資當事人之廣義解釋之下，剖析檔案、自動化決策等，係與特定當事人有關、基於其個人資料做成，除落入法定例外者外，應屬個人資料之一部，當事人得行使查閱權。

（三）查閱權的行使限制

由前述各國法律規範觀察，當事人就其個人資料享有之查閱權應非絕對，各國有不同的法益取捨與規範方式。以下將就與數位足跡關聯較為密切者個別分析。

1、蒐集機關無法識別當事人

蒐集機關未必能透過數位足跡識別特定當事人，且蒐集機關利用數位資料時，未必需要識別當事人（例如，網站自

動記錄使用者 IP 位址及其使用行為，再將其用於分析並改善網站使用狀況）。若蒐集機關就其掌握之全部資訊，無法識別數位足跡之當事人，依歐盟 GDPR，當事人得為行使其權利，向蒐集機關提供額外資訊，使其數位足跡具備辨識性，蒐集機關不得拒絕。相較之下，依美國加州 CCPA，蒐集機關並無義務為滿足當事人個資權利請求而接受或使用額外資訊。

「假名資料」可視為「無法識別當事人」之特殊情形。依美國維吉尼亞州、日本和韓國個資法律，符合條件之假名資料，被排除於查閱權行使範圍外。亦即，依此三國（州）個資法律，若蒐集機關對數位足跡進行假名化處理並符合其他法定條件，則當事人不得行使近用權。

2、過分或不合理之請求

數位足跡係使用者網路活動所產生，通常由蒐集機關自動記錄。隨著使用者活動之累積，數位足跡可能範圍廣泛、內容複雜，且單一使用者的數位足跡可能零散分布於大量數據資料之中。蒐集機關為滿足當事人查閱請求，對數位足跡進行檢索、整理、提供相關資訊等，可能需耗費較高人力、技術、財物等方面的成本。

若對於蒐集機關而言，滿足數位足跡閱覽請求之成本過高或負擔過重，美國加州 CCPA、維吉尼亞州 CDPA 與新加坡 PDPA 皆明文允許蒐集機關以勞費過鉅為由，拒絕當事人之查閱請求。歐盟 GDPR 則允許蒐集機關拒絕當事人之「過度」請求，或依滿足請求之行政成本收取合理費用。雖然歐盟 GDPR 未明確將蒐集機關滿足請求之成本列為判斷過度請求之考量要素，但成本方面之「過度」，應可作為拒絕當事

人行使權利之理由[145]。我國、日本與韓國則未見成本考量相關規範[146]。

3、對蒐集機關權益之不利影響

數位足跡之內容、紀錄方法、儲存方式、利用方式等，可能涉及蒐集機關之專有權利、營業秘密、技術秘密等。當事人就數位足跡行使查閱權，蒐集機關可否為保護自身權益而限制或拒絕當事人查閱？本報告所研究之各國個資法律都要求當事人閱覽權不得對他人權益有不利影響。其中，我國、歐盟、日本、韓國和新加坡個資法律皆明文允許蒐集機關基於對自身利益之嚴重不利影響，拒絕當事人行使閱覽權。日本、新加坡甚至明文將商業性機密資訊、競爭地位、正常經營等列為拒絕當事人行使權利之理由。

各國個資法規關於本議題之比較表格整理如下：

表 2、各國查詢閱覽權相關規範比較表

國家	權利內容	法源依據	位階
臺灣	個資當事人得就其個人資料行使「查詢或請求閱覽」之權，個資蒐集機關除有下列情形外，應答覆查詢、提供閱覽或製給複製本： (1)妨害國家安全等國家重大利益； (2)妨害公務機關執行法定職務； (3)妨害該蒐集機關或第三人之重大利益。	個人資料保護法第 3 條第 1 款、第 10 條	法律
歐盟	1、個資當事人有權向控管者確認是否	GDPR§15	法律

[145] See, e.g. UK Information Commissioner's Office, When can we refuse to comply with a request?, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/when-can-we-refuse-to-comply-with-a-request/.

[146] 應予說明者，我國、日本與韓國皆允許蒐集機關基於對自身利益之重大損害，而拒絕當事人行使查閱權。此處不考慮因成本過高而認為有損蒐集機關重大利益之情形。

國家		權利內容	法源依據	位階
		處理其個人資料。 2、控管者若處理其個人資料，個資當事人有權存取其個人資料及相關資訊，如： (1) 處理之目的； (2) 資料之類型、存儲期間、接收者； (3) 當事人權利； (4) 資料自第三方取得時，資料之來源； (5) 資料用於自動化決策之邏輯與影響。 3、控管者應就其處理之個人資料提供複製本予當事人。		
美國	加州	消費者有權要求業者提供下列資訊： (1) 蒐集其資料之類別、來源、具體內容； (2) 蒐集、銷售或分享資料之目的； (3) 資料分享之對象。	CCPA, amended by CPRA § 1798.110	法律
	維吉尼亞州	消費者有權向業者確認其是否處理個人資料，並存取該等個人資料。	CDPA § 59.1-573(A)(1)	法律
日本		個資當事人得要求資料處理者揭露其所保有的個人資料。非有下列例外情形，資料處理者不得拒絕： (1) 可能損害個資當事人或他人的生命、身體或財產利益；	個人資訊保護法 §28	法律

國家	權利內容	法源依據	位階
	(2) 可能嚴重損害資料處理者之經營； (3) 其他法令禁止揭露。		
韓國	個資當事人得向個人資料處理者要求閱覽被處理之自身個人資料。非有如下例外情形，資料處理者不得拒絕此要求： (1) 依法律禁止揭露； (2) 可能損害他人的生命、身體或財產利益； (3) 可能嚴重阻礙公務機關執行特定職務。	個人資料保護法 §35	法律
新加坡	1、 個資當事人得要求組織提供後者所保存或控制的個人資料，以及該個人資料最近一年內的利用與分享狀況。 2、 控管者得在符合法定條件時拒絕提供，包括：提供該個人資料將造成揭露機密商業資訊，以致損害組織的競爭力等。	個人資料保護法 (PDPA) §21, 5th Schedule	法律

五、修法需求分析

承繼上述法規比較，包括我國在內的各國個資法律之共通點係，具有直接或間接識別性之數位足跡，原則屬於個人資料，當事人得行使查閱權，但有限制條件。

我國個資法對於「個人資料」之定義雖不含網路活動或網路行為之相關例示，但肯認個人資料之間接識別性，並不考量蒐集機關實際取得實現識別所需其他資料之現實可行性或難易程度，也並未將公開可得之資料排除於個人資料範圍外。因此，當事人在網路上

活動或行為之紀錄，無論是否公開可得，在能夠直接或間接識別特定當事人之前提下，應屬個人資料。

然而，隨著數位技術普遍應用於日常生活各個方面，人們對網路服務和 IT 技術之依賴程度日益增加，數位足跡不再僅是人們應用網路技術之副產品，而已成為網路產業得以發展乃至獲利的核心要素之一。在此背景下，我國個資法似宜在其「個人資料」之定義中，增設有關數位足跡之相關例示，以利明確數位足跡屬於個人資料，提示業者和網路使用者依個資法蒐集處理利用數位足跡，強化當事人就數位足跡行使資料權利之保障。

參考比較法上相關規範，數位足跡之例示可透過兩種模式實現：其一為限縮性例示，即參考歐盟 GDPR 之規範，在我國個資法第 2 條第 1 款中，增設「網路識別碼」之例示，並在個資法施行細則第 4 條中，增加關於「網路識別碼」之相關舉例，例如 IP 位址、cookie、移動裝置識別碼等。

其二為廣泛性例示，即參考美國加州 CCPA 之規範，除在個資法和個資法施行細則中增加「網路識別碼」之例示及相關舉例外，一併在個資法中增加「網際網路或其他電子網路上活動或行為之資訊」，並在個資法施行細則中增加相關舉例，例如瀏覽歷史、搜尋歷史，以及與網站、應用程式或廣告之互動等。採取何種模式，宜由主管機關在擬訂相關修法草案時，參考網路業者及使用者意見作出判斷。

數位足跡可用於追蹤當事人網路活動、構建當事人剖析檔案、對當事人進行自動化決策等。我國個資法並未明文將運用數位足跡作成之剖析檔案、自動化決策等列入查閱權之行使範圍。但在有利於個資當事人之廣義解釋之下，此等如具有直接或間接識別性，應認為屬個人資料之一部，當事人得行使查閱權。惟為強化當事人就數位足跡行使資料權利之保障，我國似可增加查閱剖析檔案、自動化決策之明文。

參考比較法上相關規範，此亦可透過兩種模式實現：其一為參考美國加州 CCPA，將「剖析檔案」、「自動化決策」增列為個人資料之例示。詳言之，在我國個資法第 2 條第 1 款中，將「剖析檔案」、「自動化決策」增列為「個人資料」之例示，並在個資法施行細則中增加相應定義。其二為參考歐盟 GDPR，在個資法關於查閱權之規範中，增加查閱剖析檔案、自動化決策之明文。

考量我國個資法現行之查閱權規範，增列個人資料例示似為可行性較高之方案。然另一方面，若於個資法中新增剖析檔案、自動化決策之相關文句，必將引發我國個資法是否應新增當事人拒絕自動化決策權利之討論。

據此，剖析檔案、自動化決策之查閱權例示，宜由主管機關在擬訂相關修法草案時，與當事人拒絕自動化決策之權利作通盤考量。為求衡平當事人個人資料自主權與對我國社會行業之衝擊，本報告後文所建議之法規條文及指引草案皆採折衷方案，納入剖析檔案相關說明，及自動化決策之定義，供主管機關參考。

由於我國個資法所謂之「間接識別性」，並不要求蒐集機關具體掌握足以識別特定當事人之全部資料，由此延伸出的問題是，若對於特定間接識別性資料，蒐集機關並不掌握足以識別當事人之全部資料（亦即，蒐集機關無法透過該間接識別性資料識別特定當事人），當事人可否、以及如何對該間接識別性資料行使當事人權利。特別地，此種情形下，蒐集機關是否有義務接受當事人提供之額外身分辨識資訊，以使當事人行使其當事人資料權利？於數位足跡而言，此一問題尤其有相關性。

我國個資法對此並無明確規範。比較法上，歐盟 GDPR 和美國加州 CCPA 對此訂有明確規則。兩者皆規定，若蒐集機關不需要識別特定當事人即可蒐集處理利用其個人資料，則蒐集機關並無義務為識別當事人而取得額外資訊。

但在行使當事人資料權利方面，兩者立場相反：歐盟 GDPR 對此訂有例外條款，規定當事人為行使其資料權利而提供額外資訊，

使該間接識別性資訊足以被辨識者，蒐集機關不得拒絕。相較之下，美國加州 CCPA 則並無類似例外，而是明文規定蒐集機關並無義務蒐集、取得、保存或近用任何數據或技術，以便當事人就該間接識別性資訊行使其資料權利。

歐盟 GDPR 與美國加州 CCPA 在此一問題上的差異，反映的是歐盟與美國加州立法者在消費者資料權利保障程度方面的政策選擇。在蒐集機關無法透過某一間接識別性資料識別特定當事人時，若要求其有義務為滿足當事人權利行使請求而取得額外資訊，恐對於蒐集機關課予不適當的負擔，因此 GDPR 與 CCPA 皆規定蒐集機關並無取得額外資訊之義務。但 GDPR 在當事人（主動）提供該額外資訊時，雖仍將額外增加蒐集機關就原本持有之資料於該額外資訊進行對照、組合、連結等之負擔，但相較於為滿足當事人請求而自其他管道尋求該額外資訊，可認蒐集機關之負擔已大大降低。

惟是否為保障當事人之資料權利，而對蒐集機關課予此相對較低之額外負擔，歐盟與美國加州之立法者作出了不同選擇。如本節前文比較法分析所示，此一問題在國際上尚未形成一致之處理方式。因此，我國似可先對此問題繼續觀察研究，由個資法主管機關基於對我國個資保護法制需求之整體分析，於時機適當時提出修法草案。

六、本節結論

綜合本節比較研究，本報告發現，包括我國在內的各國個資法律之共通點係，具有直接或間接識別性質數位足跡，原則屬於個人資料，當事人得行使查閱權，但有限制條件。為明確數位足跡屬於個人資料，提示業者和網路使用者依個資法蒐集處理利用數位足跡，強化當事人就數位足跡行使資料權利之保障，我國似可考慮在個資法或其施行細則中關於「個人資料」之條文，增列數位足跡之相關例示。

第三節 告知目的外利用或利用開放資料為自動化決策

一、議題釐清

本議題源於「臺灣開放政府國家行動方案」中的承諾事項 1-3「強化數位隱私與個資保護」[147]，基於「現行個資法對直接或間接蒐集個資之告知設有相關規定，惟針對『特定目的外』或『利用開放資料經自動化處理做成決定』等情形，皆未要求告知」，是本議題擬就「目的外利用」及「利用開放資料經自動化處理做成決定」等情形之告知要件及配套措施之可行性，進行研議。

需先敘明者，在「利用開放資料經自動化處理做成決定」方面，由於開放資料並非於我國個資法所規定，在我國實務上，開放資料應係指非個人資料或已無從識別特定當事人之資料，因此，本議題的關注焦點應非置於蒐集者額外取得開放資料，而應關注蒐集者以另行取得的開放資料，與其保有的當事人個人資料透過演算法等方式比對、分析後，所對當事人自動作成決策，個資法是否應課予蒐集者向當事人揭露該行為之義務。

二、我國個人資料保護法

我國個資法於第 8 條及第 9 條分別針對「直接蒐集」與「間接蒐集」行為，課予蒐集者向當事人揭露特定資訊的告知義務，然而，對於蒐集者在蒐集目的之外，為其他目的利用個人資料之行為，僅於第 16 條但書針對公務機關、第 20 條第 1 項但書針對非公務機關，定有合法目的外利用個人資料之事由，其中除以「經當事人同意」為依據時，依個資法第 7 條第 2 項規定，須先向當事人告知目的、範圍等資訊外，個資法並未規範蒐集者在目的外利用個人資料時，有義務向當事人告知特定法定事項。

而在自動化決策方面，蒐集者利用當事人之個人資料（與其他資料—例如開放資料—比對分析）而對其作成自動化決策，本質上

[147] 臺灣開放政府國家行動方案，2021 年 4 月，頁 12-15。

可視為利用個人資料之行為，似應落入個資法第 8 條第 1 項第 4 款的告知義務範圍（利用方式）。

三、外國立法例

（一）歐盟 GDPR

歐盟 GDPR 第 13 條第 3 項規定[148]，在控管者自當事人直接蒐集個人資料的情形，當控管者有意將個人資料為目的外利用時[149]，應於目的外利用之前，向當事人提供該目的之資訊，以及該條第 2 項所列的相關進一步資訊，除非應告知之資訊已為當事人所知（第 4 項）[150]。

第 14 條第 4 項亦規定[151]，在控管者間接蒐集個人資料的情形，控管者有意將個人資料為目的外利用時，應於目的外利用之前，向當事人提供該目的之資訊，以及該條第 2 項所列的相關進一步資訊，但有下列事由者不在此限[152]：(1) 應告知之資訊已為當事人所知；(2)證明不可能告知資訊，或須投入不成比例的付出始得告知資訊，特別是在符合 GDPR 第 89

[148] EU, GDPR, §13(3), "Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2."

[149] 條文用語為"further process"，直譯為「進階處理」，性質同我國個資法下的特定目的外利用。為求用語一致以便於理解，此處譯為「目的外利用」。

[150] EU, GDPR, §13(4), "Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information."

[151] EU, GDPR, §14(4), "Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2."

[152] EU, GDPR, §14(5), "Paragraphs 1 to 4 shall not apply where and insofar as: (a) the data subject already has the information; (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available; (c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy."

條第 1 項（安全維護措施）的前提下，為公共利益、科學或歷史研究目的或統計目的而建檔等目的之處理行為。在此情形，控管者應採取適當措施保護當事人的權利、自由與正當利益，包含將應告知之資訊公諸於眾；(3)控管者受拘束的歐盟或會員國法律明文規定應揭露個人資料，且該法亦規範適當措施以保護當事人的正當利益；(4)依歐盟或會員國法律規定，該個人資料為職業秘密而應予保密。

而在自動化決策方面，GDPR 第 22 條第 1 項和第 4 項規定當事人有權不受對其產生法律效果或類似重大影響之純自動化決策（包含剖析）所拘束。

GDPR 第 13 條第 2 項第 f 款和 14 條第 2 項第 g 款皆規定，為確保公平透明之處理，控管者於直接或間接蒐集當事人個人資料時，應向當事人告知是否存在 GDPR 第 22 條第 1 項和第 22 條第 4 項所述之自動決策資訊（包括剖析），以及（至少在存在自動化決策時）與所涉邏輯相關之有意義資訊，和處理對當事人之重要性和預期後果[153]。GDPR 前言第 71 點更指出，控管者在以個人資料為自動化決策時，須採取適當的安全措施，包含向當事人告知經評估後作成該決策之原因[154]。

第 29 條個資保護工作小組 (Article 29 Data Protection Working Party, WP29) 指引說明，GDPR 第 13 條和第 14 條要求控管者以簡單而清晰之方式，向當事人說明剖析或自動化決策程序之運作。GDPR 要求告知「所涉邏輯相關之有意義資訊」，並非要求完整揭露所使用之演算法、或提供複雜解

[153] EU, GDPR, §13(2): "In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: … (f): the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."

[154] EU, GDPR, Recital§71, paragraph 4: "In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision."

釋，而是要求簡明地告知當事人決策背後之基本原理，或達成決策之標準，以使當事人瞭解所作決策之理由。而「處理對當事人的重要性和預期後果」係指對當事人的潛在影響。為了使這些資訊有意義且可理解，應提供可能影響類型之真實、確切之示例。[155]

據此，若控管者在蒐集個人資料時已知該資料將被用於自動化決策（包括剖析），則應向當事人告知自動化決策相關資訊。若控管者計劃對已蒐集之個人資料為目的外利用，且該目的外利用涉及自動化決策，則依 GDPR 第 13 條第 3 項（直接蒐集）或 14 條第 4 項（間接蒐集），控管者應於目的外利用前，向當事人告知自動化決策相關資訊。告知自動化決策相關資訊之例外，適用 GDPR 第 13 條第 4 項（直接蒐集）或第 13 條第 5 項（間接蒐集）之規範。

WP29 指引說明，若控管者基於剖析而進行決策，則無論是否適用 GDPR 第 22 條關於自動化決策之規範，控管者皆應向當事人明確告知(a)決策以及(b)基於該剖析而進行決策。若自動化決策和剖析不符合第 22 條之定義，提供自動化決策邏輯及後果之相關資訊，亦屬一種優良實務做法[156]。

（二）美國加州 CCPA

CCPA 第 1798.100 條第 a 項規定[157]，企業如蒐集個人資訊者，應在蒐集時或蒐集前，向消費者告知特定資訊（個人資

[155] WP29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (6 February 2018) 47-49.

[156] WP29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (6 February 2018) 29, 47.

[157] California, CCPA, §1798.100(a), “A business that controls the collection of a consumer’s personal information shall, at or before the point of collection, inform consumers of the following:(1) The categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected without providing the consumer with notice consistent with this section.(2) If the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared. A business shall

訊類別、蒐集或利用個人資訊之目的，以及該資訊係購得或由他人分享而得）。

其中，第1款（針對一般個人資訊）與第2款（針對敏感個人資訊）均規定，業者若未向消費者依本條規定通知資訊，不得將已蒐集之個人資訊用於與其揭露之蒐集目的不相容（incompatible）的其他目的。

在自動化決策方面，依修正後的 CCPA 第 1798.185 條第 a 項第 16 款，州檢察長應制定施行細則，規定業者使用自動化決策技術（包括剖析）處理個人資料時，消費者之近用權和拒絕權。施行細則之內容應包括，業者對消費者近用請求之回覆，應提供關於決策邏輯之有意義的資訊，並描述該處理對消費者可能造成之後果[158]。由 CCPA 整體架構觀之，此應係要求州檢察長就自動化決策（包括剖析）所涉個資處理，制定同法第 1798.110 條（近用權）和第 1798.120 條（拒絕權）之細部規範。該修正條文自 2020 年 12 月生效，但截至 2021 年 11 月，加州州檢察長尚未公布相關施行細則。雖此一規範並無加州州檢察長應以施行細則要求業者向消費者主動告知自動化決策技術（包括剖析）之使用狀況及後果，然拒絕權之行使係以知悉自動化決策（包括剖析）之存在為前提，故未來加州如頒行消費者自動化決策拒絕權施行細則，預估其內容應將涉及向消費者之告知事宜。

---

not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected without providing the consumer with notice consistent with this section.(3) The length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose."

[158] California, CCPA (as amended by CPRA) 1798.185(a), "On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas: … (16) Issuing regulations governing access and opt-out rights with respect to businesses' use of automated decision making technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decision making processes, as well as a description of the likely outcome of the process with respect to the consumer.

（三）美國維吉尼亞州 CDPA

CDPA 第 59.1-574 條第 A 項第 2 款規定[159]，除 CDPA 另有規定外，控管者非得消費者同意，不得為「與其向消費者揭露之蒐集目的既不合理必要（reasonably necessary）也不相容（compatible）」之目的而處理個人資料。

另維吉尼亞州 CDPA 並未規定個資當事人拒絕自動化決策之權利，亦未就自動化決策之告知或近用權作出特別規範。

（四）日本個人資訊保護法

依日本個人資訊保護法第 16 條第 1 項與第 3 項規定，除非符合例外事由，個人資訊處理事業非事先得到當事人之同意，不得逾越特定利用目的必要範圍，處理個人資訊。

然而，日本個人資訊保護法第 15 條第 2 項允許個人資訊處理事業在與原始利用目的有合理關聯的範圍內，變更利用目的。此時，依第 18 條第 3 項規定[160]，個人資訊處理事業如變更資料之利用目的，應將變更後之目的通知當事人或公諸於眾，但同條第 4 項列出 4 款不適用前項義務的事由[161]：

1、 通知可能損害當事人或他人的生命、身體或財產利益；

2、 通知可能嚴重損害資料處理者之權利或正當利益；

3、 依法令配合公務機關執行職務，揭露可能妨礙執行該職務；

[159] Virginia, CDPA, §59.1-574(A)(2), “A controller shall:…2. Except as otherwise provided in this chapter, not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent”.

[160] 日本，個人情報保護法，§18(3),「個人情報取扱事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。」

[161] 日本，個人情報保護法，§18(4),「前三項の規定は、次に掲げる場合については、適用しない。一　利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合。二　利用目的を本人に通知し、又は公表することにより当該個人情報取扱事業者の権利又は正当な利益を害するおそれがある場合。三　国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。四　取得の状況からみて利用目的が明らかであると認められる場合。」

4、從資料蒐集情形可顯見利用目的。

至於自動化決策方面，日本個資保護法律並未規定個資當事人拒絕自動化決策之權利，亦未就自動化決策之告知或近用權作出特別規範。

經配合數位社會整備法修正後，前開規範雖有條號及文字調整，但其內容並無實質變化。

（五）韓國個人資料保護法

韓國個人資料保護法第 15 條第 2 項規定[162]，當個人資料處理者以「取得當事人同意」作為蒐集、利用個人資料之合法要件時，應向當事人告知下列資訊，如日後有任何變更時，應再向當事人告知並取得同意：(1)個人資料的蒐集與利用目的；(2)蒐集個人資料之項目（義同類別）；(3)保有及利用個人資料的期間；(4)有權利拒絕同意之事實，以及拒絕同意如將受不利益時，該不利益之內容。

另依韓國個人資料保護法第 17 條第 2 項規定[163]，個人資料處理者以「取得當事人同意」作為將個人資料提供予第三方（包含共同利用）的合法要件時，應向當事人告知下列資訊，如日後有任何變更時，應再向當事人告知並取得同意：(1)個人資料之接收者；(2)個人資料接收者利用該個人資料之

[162] 한국，개인정보보호법，§15(2)，「개인정보처리자는 제 1 항제 1 호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다. 1. 개인정보의 수집·이용 목적 2. 수집하려는 개인정보의 항목 3. 개인정보의 보유 및 이용 기간 4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용」。

[163] 한국，개인정보보호법，§17(2)，「개인정보처리자는 제 1 항제 1 호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다. 1. 개인정보를 제공받는 자 2. 개인정보를 제공받는 자의 개인정보 이용 목적 3. 제공하는 개인정보의 항목 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용」。

目的；(3)提供個人資料的項目（義同類別）；(4)個人資料接收者保有及利用該個人資料的期間；(5)有權拒絕同意之事實，以及拒絕同意如將受不利益時，該不利益之內容。

又依韓國個人資料保護法第 18 條第 2 項第 1 款規定[164]，個人資料處理者如自當事人取得別途同意[165]，可於蒐集目的外利用個人資料或提供予第三方。此時，同條第 3 項規定[166]，個人資料處理者應向當事人告知下列資訊，如日後有任何變更時，應再向當事人告知並取得同意：(1)個人資料接收者；(2)個人資料之利用目的（於提供第三方之情形，接收者於接收時之利用目的）；(3)被利用或被提供的個人資料項目（義同類別）；(4)保有及利用個人資料的期間（於提供第三方之情形，接收者於接收時之保有及利用期間）；(5)有權拒絕同意之事實，以及拒絕同意如將受不利益時，該不利益之內容。

除前述「當事人同意之事項有變更（包含目的變更），即須告知該變更並取得同意」，以及第 18 條第 2 項第 1 款「向當事人告知法定事項後取得別途同意」等規定外，韓國個人資料保護法第 18 條第 2 項尚列舉其他得於目的外利用個

---

164 한국，개인정보보호법，§18(2)，「제 1 항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제 3 자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제 3 자에게 제공할 수 있다. 다만, 이용자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제 2 조제 1 항제 4 호에 해당하는 자를 말한다. 이하 같다)의 개인정보를 처리하는 정보통신서비스 제공자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제 2 조제 1 항제 3 호에 해당하는 자를 말한다. 이하 같다)의 경우 제 1 호・제 2 호의 경우로 한정하고, 제 5 호부터 제 9 호까지의 경우는 공공기관의 경우로 한정한다. 1. 정보주체로부터 별도의 동의를 받은 경우」。

165 별도的漢字為「別途」，即另外用途、其他用途之意，此應指目的外利用個人資料之同意。

166 한국，개인정보보호법，§18(3)，「개인정보처리자는 제 2 항제 1 호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다. 1. 개인정보를 제공받는 자 2. 개인정보의 이용 목적(제공 시에는 제공받는 자의 이용 목적을 말한다) 3. 이용 또는 제공하는 개인정보의 항목 4. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다) 5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용」。

人資料或提供個人資料予第三方的合法要件[167]，包含(1)其他法律有特別規定之情形；(2) 當事人及其法定代理人陷於無法為意識表示之狀態，或住所不明等而無法取得事前同意，確實有明顯對當事人及第三方急迫生命、身體、財產利益所必要時；(3)若不得於目的外利用或向第三方提供個人資料，將致公務機關無法執行其他法律已規定之業務職責時，保護委員會以審議、議決為表決；(4)公務機關為履行條約、其他國際協議，而有對外國政府或國際組織提供之必要；(5)為犯罪之搜查與公訴之提起及維持所必要；(6)法院為執行裁判職務所必要；(7)為執行刑罰及監護、保護處分所必要。

此時，如係公務機關欲於目的外利用或提供個人資料予第三方者，除為犯罪之搜查與公訴之提起及維持所必要外，依第 18 條第 4 項規定[168]，保護委員會應告示（即國家機關發

[167] 한국，개인정보보호법，§18(2)，「제 1 항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제 3 자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제 3 자에게 제공할 수 있다. 다만, 이용자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제 2 조제 1 항제 4 호에 해당하는 자를 말한다. 이하 같다)의 개인정보를 처리하는 정보통신서비스 제공자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제 2 조제 1 항제 3 호에 해당하는 자를 말한다. 이하 같다)의 경우 제 1 호・제 2 호의 경우로 한정하고, 제 5 호부터 제 9 호까지의 경우는 공공기관의 경우로 한정한다. 1.정보주체로부터 별도의 동의를 받은 경우 2. 다른 법률에 특별한 규정이 있는 경우 3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제 3 자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 4. 삭제 5. 개인정보를 목적 외의 용도로 이용하거나 이를 제 3 자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의・의결을 거친 경우 6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우 7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우 8. 법원의 재판업무 수행을 위하여 필요한 경우 9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우」。

[168] 한국，개인정보보호법，§18(4)，「공공기관은 제 2 항제 2 호부터 제 6 호까지, 제 8 호 및 제 9 호에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제 3 자에게 제공하는 경우에는 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 보호위원회가 고시로 정하는 바에 따라 관보 또는 인터넷 홈페이지 등에 게재하여야 한다.」

布以向一般人告知）該利用或提供個人資料之合法要件、目的及範圍等相關必要事項，並刊登於政府公報或官方網站上。

而在自動化決策方面，韓國現行個人資料保護法並未規定個資當事人拒絕自動化決策之權利，亦未就自動化決策之告知或近用權作出特別規範。然韓國個人資料保護委員會於2021 年 1 月公告個人資料保護法修正案草案並公開徵求意見[169]。該修正案草案計劃新增個資當事人拒絕自動化決策之權利。

（六）新加坡個人資料保護法

依新加坡個人資料保護法第 18 條第 b 款規定[170]，組織僅得為「已依第 20 條規定向當事人告知」之目的，蒐集、利用或揭露個人資料。第 20 條第 1 項第 a 款要求組織於蒐集時或蒐集個人資料前，向當事人告知蒐集、利用或揭露該個人資料之目的。同項第 b 款則規定，組織在為任何新目的利用或揭露當事人之個人資料前，應向當事人告知該「尚未依該項第 a 款向當事人告知」之目的[171]。

但依第 20 條第 3 項規定[172]，若當事人依本法規定「經通知視為同意」蒐集、利用或揭露行為，或組織依本法規定得

[169] 개인정보보호위원회，「개인정보 보호법」일부개정법률(안)입법예고（2021.01.06），https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS061&mCode=C010010000&nttId=7059#LINK。

[170] Singapore, PDPA, §18(b), “An organisation may collect, use or disclose personal data about an individual only for purposes — (b) that the individual has been informed of under section 20, if applicable.”

[171] Singapore, PDPA, §20(1) , “For the purposes of sections 14(1)(a) and 18(b), an organisation shall inform the individual of —(a) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data; (b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph (a), before the use or disclosure of the personal data for that purpose…”

[172] Singapore, PDPA, §20(3), “Subsection (1) shall not apply if — (a) the individual is deemed to have consented to the collection, use or disclosure, as the case may be, under section 15 or 15A; or (b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17. ”

以其他合法要件，「不須取得當事人同意」即可蒐集、利用或揭露個人資料時[173]，前述「告知義務」即不適用。

又新加坡 PDPA 並未規定個資當事人拒絕自動化決策之權利，亦未就自動化決策之告知或近用權作出特別規範。

四、法規比較

由上述法規比較可知，在目的外利用個人資料的告知義務方面，歐盟與美國加州、維吉尼亞州有較嚴格的規範。歐盟 GDPR 對控管者的目的外利用個資（進階處理）行為，仍要求以「向當事人告知」為原則，配合特定例外以平衡控管者履行告知義務的成本；美國加州 CCPA 則規定業者若未向消費者告知，即不得將已蒐集之個人資訊用於其他目的；維吉尼亞州 CDPA 亦規定，非得消費者同意，控管者不得為「與其向消費者揭露之蒐集目的既不合理必要也不相容」之目的而處理個人資料。

而日本個人資訊保護法允許個人資訊處理事業在與原利用目的有合理關聯的範圍內，任意變更利用目的，但原則上應將變更後之目的通知當事人或公諸於眾；韓國個人資料保護法則要求公務機關除經當事人同意，或為犯罪之搜查與公訴之提起及維持所必要外，縱使符合例外而得於目的外利用個人資料，保護委員會亦應告示該利用或提供個人資料之合法要件、目的及範圍等相關必要事項，並刊登於政府公報或官方網站。

新加坡個人資料保護法則允許若當事人依該法規定「經通知視為同意」組織的蒐集、利用或揭露行為，或組織依該法規定得以其他合法要件，「不須取得當事人同意」即可蒐集、利用或揭露個人資料時，組織為新目的利用個人資料即無須向當事人告知。

[173] 例如為當事人或第三人的重大利益、為影響公眾之事、為組織或第三人的正當利益、為商業資產交易、為商業優化目的、依公務機關公開個人資料之目的而蒐集或利用、為明確的公共利益而有研究必要，並不以研究結果對當事人做成任何決定，且該結果若公開，須無從識別當事人身分等。詳見新加坡個人資料保護法，附表 1 與附表 2。

又在自動化決策方面，歐盟 GDPR 要求控管者在蒐集資料時即應向當事人告知自動化決策之資訊；美國加州 CCPA 則規定由州檢察長應制定施行細則，規範業者使用自動化決策技術（包括剖析）處理個人資料時，消費者之近用權和拒絕權；韓國個人資料保護委員會於 2021 年 1 月公告個人資料保護法修正案草案並公開徵求意見，計劃新增個資當事人拒絕自動化決策之權利。2021 年 9 月，韓國再行公布自動化決策拒絕權之修法草案，但並未就自動化決策之告知作出特別規範。考量拒絕權之行使係以知悉所拒絕行為之存在為前提，且自動化決策（包括剖析）因其技術性與隱秘性，其存否並非當事人易於獲知之資訊，故可合理推測，前開自動化決策拒絕權之規範中，將包含一定形式之告知義務。

各國個資法規關於本議題之比較表格整理如下：

表 3、各國個資目的外利用告知相關規範比較表

國家		權利內容	法源依據	位階
臺灣		以「當事人同意」作為個資目的外利用之依據時，在目的外利用前須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。	個人資料保護法第 7 條第 2 項	法律
歐盟		控管者如欲目的外利用(進階處理)個人資料，則應在目的外利用前，向個資當事人告知處理目的、當事人權利等。	GDPR§13(3)	法律
美國	加州	業者在向消費者告知法定事項前，不得將已蒐集之個人資料用於與蒐集時所揭露者不相容之目的。	CCPA, amended by CPRA §1798.100(a)	法律

國家		權利內容	法源依據	位階
	維吉尼亞州	控管者應以清晰、明白且可合理獲得的隱私聲明，告知個人資料之處理目的及其他內容。	CDPA §59.1-573	法律
日本		個資處理者變更資料之利用目的者，應通知個資當事人，但下列情形除外： (1)通知可能損害個資當事人或他人的生命、身體或財產利益； (2)通知可能嚴重損害資料處理者之權利或正當利益； (3)依法令配合公務機關執行職務，揭露可能妨礙執行該職務； (4)從資料蒐集情形可顯見利用目的。	個人資訊保護法 §18	法律
韓國		1、個資處理者不得對個人資料作目的外利用，但個資當事人同意目的外利用或法律另有規定者除外。 2、取得當事人同意時，須告知利用目的。	個人資料保護法 §§15(2), 18	法律
新加坡		1、組織在蒐集個人資料時或在此之前，須先將蒐集、利用或揭露該資料之目的告知個資當事人。 2、組織須在目的外利用前，須先將該目的告知當事人。	PDPA §20(1)(b)	法律

五、修法需求分析與本節結論

雖然比較法規對於目的外利用個人資料的告知義務規範不盡相同，但由於目的外利用個人資料之行為，本質上即超出當事人的隱私期待，對當事人的資訊隱私權（自主權）影響更鉅，我國現行個資法並未課予蒐集者在目的外利用個人資料前，評估向當事人揭露該新目的之原則與例外的義務，似有調整空間。

退步言之，在個資法第 8 條、第 9 條已對蒐集者明定於蒐集個人資料時應負擔告知義務與例外的情形下，倘蒐集者於蒐集時無例外事由而須向當事人告知特定資訊，則在該蒐集者於原始蒐集目的之外利用個人資料時，反倒一律無須承擔告知義務，恐有輕重失衡之虞。

本報告據此認為，個資法宜適當導入目的外利用個人資料的告知義務之原則與例外規範，一方面賦予當事人知情機會，另方面平衡考量當事人的權利受限程度與蒐集者目的外利用個人資料所追求之目的，建構權利保障與合理利用個人資料之框架。此修法方向可由兩方面著手，其一為參考個資法第 8 條與第 9 條對於蒐集時告知義務的例外規定，移植適當例外條款適用於目的外利用個人資料情形；其二則係依個資法第 16 條與第 20 條所列得目的外利用個人資料之事由，逐一檢視應否就個別情形課予蒐集者於目的外利用個人資料時的告知義務。

至於自動化決策之告知與否，由於此行為可視為利用個人資料之方式之一，應屬於個資法第 8 條第 1 項第 4 款的告知義務範圍，歐盟 GDPR 獨立對此訂定規範，毋寧認為係因 GDPR 賦予當事人對自動化決策的拒絕權，是特別要求控管者應向當事人揭露自動化決策之事實與當事人可拒絕之權利。

因此本報告認為，此處應與本章第一節拒絕權之增訂一併評估，如於我國個資法新增當事人對於自動化決策之拒絕權，即應一同強調蒐集機關對當事人揭露自動化決策之事實的義務。

第四節 個資外洩通知

一、議題釐清

本議題源於「臺灣開放政府國家行動方案」中的承諾事項 1-3「強化數位隱私與個資保護」[174]，欲探究者為「現行個資法雖有規定當個資侵害發生時，應查明後以適當方式通知當事人，惟通知當事人之方式、項目等尚未有明確規定，是否可透過指引等方式說明，以供各界參考」。對此，本議題即須特別針對「為有效控制損害之擴大，針對包括個資被竊取、洩漏等侵害事件發生時，如何通知當事人及通知當事人之項目」進行研議。

個人資料侵害事故發生時之通知，可分為兩個面向：向受影響的當事人之通知，以及向主管機關之通報。據此，本報告除檢視我國及國外法制關於通知當事人方式及項目之規範外，亦會討論侵害事故是否通報主管機關、通報條件如何。

二、我國個人資料保護法

我國個資法第 18 條和第 27 條第 1 項分別要求公務機關及非公務機關應採行安全維護措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。個資法施行細則第 12 條第 2 項第 4 款說明，該等安全維護措施包括事故之預防、「通報」及應變機制。

（一）通知當事人

個資法第 12 條規定，公務機關或非公務機關違反本法規定，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。依個資法施行細則第 22 條第 1 項，所謂「適當方式通知」，係指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但書規定允許在通知需費過鉅時，

[174] 臺灣開放政府國家行動方案，2021 年 4 月，頁 12-15。

「斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之」。同條第 2 項係關於通知內容之要求，通知「應包括個人資料被侵害之事實及已採取之因應措施」。

據此，我國個資法所定強制通知當事人之情境，係侵害事故發生機關「違反個資法規定」，並因此「致使」個資侵害事故發生。依主管機關之見解，「違反個資法」之具體規定為何，並未限制；且事故發生機關是否有違反個資法規定，致個人資料被竊取、洩漏、竄改或其他侵害，係屬事實認定。於需時查明而無法立即確認時，為保障當事人權益，應使該個人資料之當事人能知曉其個人資料已被竊取、洩漏、竄改或其他侵害之情形，不待事故發生機關違法情事已明確認定[175]。此外，事故發生機關縱已依個資法辦理安全維護事項，亦不免除個資侵害事故之通知責任[176]。

除前開侵害事故通知規範外，個資法第 27 條授權中央目的事業主管機關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，並就該等安全維護計畫及處理方法之標準等相關事項，制定管理辦法。觀察目前各中央目的事業主管機關已頒行之管理辦法可知，目的事業主管機關可能要求指定非公務機關制定相關機制，於個資侵害事故發生後通知當事人，似不以該侵害事故係該非公務機關違反個資法所致為限。且對於通知之內容，也可能有其他要求。例如，金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法第 6 條規定，金融服務業為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故，應訂定查明事故後通知當事人之適當方式，以及應通知當事人事故事實、所為因應措施及諮詢服務專線等內容。

[175] 見法務部 106 年 6 月 5 日法律字第 10603503230 號函。
[176] 見法務部 106 年 1 月 26 日法律字第 10503517710 號函。

（二）通報主管機關

我國個資法並無個資侵害事故通報主管機關之明文規範，雖如前所述，依個資法施行細則第 12 條第 2 項第 4 款，個資侵害事故之通報係個資安全維護措施之一，惟在實務上，此「通報」對公務機關或非公務機關而言，似均解釋為機關的「內部」通報措施。

就公務機關而言，個人侵害事故之通報，多透過內部個人資料管理保護管理制度加以規範。例如，《法務部個人資料保護管理要點》、《教育部個人資料保護管理要點》等皆於機關內部設置收受個資侵害事故之專門窗口，並於《資通安全管理法》通過並施行後，要求個資侵害事故之通報，遵循資通安全事件通報管道處理。

就非公務機關而言，個資法雖未要求個資侵害事故通報主管機關，但中央目的事業主管機關可能對管轄範圍內之非公務機關訂有個資侵害外洩通報規範，且各中央目的事業主管機關訂定之通報範圍、時限、受理通報之機關層級等不盡一致，其中至少包括：

1、通報重大個資侵害事故至中央目的事業主管機關

依金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法第 6 條、經濟部網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法第 8 條，以及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第 4條，金融服務業者、網際網路零售業者、通訊傳播業者遇有重大個人資料事故，應分別通報金融監督管理委員會、經濟部或國家通訊傳播委員會。所謂重大事故，係

指個人資料遭竊取、竄改、毀損、滅失或洩漏，將危及相應業者正常營運或大量當事人權益之情形。

2、通報各類個資侵害事故至直轄市、縣（市）主管機關

依教育部所訂短期補習班個人資料檔案安全維護計畫實施辦法第 13 條，補習班應於發生個人資料被竊取、洩漏、竄改或其他侵害事故時，查明事故發生原因及損害狀況，通報其直轄市、縣（市）主管機關。

3、限期通報各類事故至直轄市、縣（市）主管機關

依教育部所訂私立兒童課後照顧服務中心個人資料檔案安全維護計畫實施辦法第 15 條，課照中心在發生個人資料被竊取、洩漏、竄改或其他侵害事故時，應查明事故發生原因及損害狀況，並於事件發生之日起「三日內」，通報其直轄市、縣（市）主管機關；並自處理結束之日起一個月內，將處理方式及結果，報主管機關備查。

為督促各中央目的事業主管機關落實監管所轄事業之個人資料保護事宜，行政院於 110 年 8 月 11 日函頒「行政院及所屬各機關落實個人資料保護聯繫作業要點」，明定強化監管措施。該要點第 4 點第 1 項第 3 款敘明，「非公務機關個資外洩時，依安全維護辦法應通報之對象、時點、應通報事項、後續行政檢查等事項；其通報地方目的事業主管機關者，並應副知中央目的事業主管機關」。因應此一要求，中央各部會已先後訂定或修正並發布人力仲介業個人資料檔案安全維護計畫及處理辦法、內政部指定警政類非公務機關個人資料檔案安全維護管理辦法等規範，採通報所在地之直轄市、縣（市）政府，並副知中央目的事業主管機關。

三、外國立法例

（一）歐盟 GDPR

GDPR 在歐盟法中引入了個人資料侵害通報主管機關及通知當事人之制度。個人資料侵害通報與通知制度係控管者應採取之組織性及制度性技術之一部分。依 GDPR 第 4 條第 12 款之定義[177]，所謂「個人資料侵害」，係指導致所傳輸、儲存或以其他方式處理之個人資料遭意外或非法破壞、遺失、變更、未經授權揭露或存取之安全侵害。前言第 87 點說明，控管者應採取一切適當之技術保護與組織措施，以便立即確定個人資料侵害是否發生，並事故發生時迅速通報主管機關、通知個資當事人。

1、通知當事人

依 GDPR 第 34 條，發生個人資料侵害事故後，控管者須在符合特定條件時，通知受影響之個資當事人。具體而言，於個人資料侵害可能導致自然人權利和自由之高風險時，控管者應與個資當事人就個人資料侵害進行溝通，不得無故延遲[178]。控管者於通知當事人時，應以簡明之語言提供侵害性質之描述，並至少包括：(1)個資保護長或其他聯絡窗口之姓名（名稱）和聯繫方式；(2)侵害可能之後果的描述，以及(3)控管者採取或預計採取之侵害因應措施的描述，適當情形下，包括為減輕可能之不利影響而採取之措施[179]。

[177] EU, GDPR, §4(12), "'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;…".

[178] EU, GDPR, §34(1), "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."

[179] EU, GDPR, §34(2), "The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)."; §33(3), "The notification referred to in paragraph 1 shall at least:… (b) communicate the name and contact details

依 WP29 指引，原則上，控管者應直接與受影響的當事人溝通，且為確保溝通清晰明瞭，侵害事故通知應單獨發送，而不應與其他資訊一併發送[180]。

GDPR 第 34 條第 3 項列舉了控管者無需通知當事人之情形[181]，包括：(1)控管者已採取適當的技術性與組織性措施保護受影響的個人資料，特別是使未獲授權存取之人無法解讀個人資料之措施，例如加密措施。WP29 指引說明，此等技術性與組織性措施應係侵害發生前採取的措施。(2)侵害發生後，控管者已採取措施確保個人權利和自由之高風險已不再可能實現。WP29 指引說明，此等措施應於侵害發生後立即採取。(3)與當事人溝通將勞費過鉅，此時控管者應採取公共溝通或其他替代方式，以便當事人同樣有效地獲得通知。依據 GDPR 第 5 條第 2 項規定的課責原則，控管者若未通知當事人，則需能夠向主管機關證明其符合前述規範。但 WP29 提醒，即使在侵害事故發生之初，可能因為對自然人的權利和自由無風險而不需通知個資當事人，但隨著時間推移，風險可能發生變化，因而須要重新評估風險[182]。

---

of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects."

[180] WP29, Guidelines on Personal data breach notification under Regulation 2016/679 (6 February 2018).

[181] EU, GDPR, §34(3), "The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner."

[182] WP29, Guidelines on Personal data breach notification under Regulation 2016/679 (6 February 2018) 22.

主管機關得對控管者對當事人之通知提出要求或建議。依 GDPR 第 34 條第 4 項[183]，若控管者尚未就個人資料侵害事故通知當事人，主管機關得考量事故造成高風險之可能性，要求控管者通知當事人，或判定符合第 34 條第 3 項所列條件而無需通知當事人。GDPR 前言第 86 點說明，在通知當事人方面，控管者應與主管機關密切合作，並尊重主管機關或其他機關（例如執法機關）提供的指導。例如，若需採取適當措施以因應持續的或類似個人資料侵害，則可作為較長溝通時間的正當化理由。前言第 88 點說明，侵害通知之形式與程序應考量執法機關之正當利益，過早揭露侵害事故可能會對個人資料侵害情形之調查造成不必要的妨礙。

個人資料侵害事故是否可能導致自然人權利和自由的「高風險」，係判斷是否通知當事人之關鍵。GDPR 前言第 75 點和第 76 點說明，風險評估應以客觀為基礎，考量當事人之權利和自由所受風險的可能性和嚴重性。依 WP29 指引，在評估侵害事故可能導致的風險時，控管者應考慮侵害之具體情況，包括潛在影響的嚴重程度以及該影響發生的可能性，具體考量要素可能包括侵害事故的類型，個人資料之性質、敏感性和數量，辨識當事人之容易程度，對當事人潛在影響之嚴重性，當事人及控管者之特性，受影響當事人之數量等[184]。

2、 通報主管機關

[183] EU, GDPR, §34(4), "If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met."

[184] WP29, Guidelines on Personal data breach notification under Regulation 2016/679 (6 February 2018) 24-26.

依 GDPR 第 33 條第 1 項[185]，發生個人資料侵害事故時，控管者應立即通報主管機關，控管者至遲應於知悉該事故後 72 小時內通報主管機關，但侵害事故幾乎不致（unlikely）影響個資當事人權利與自由者，不在此限。

與通知當事人相比，GDPR 要求通報主管機關之門檻更低。侵害事故發生後，控管者原則應通報主管機關，除非該侵害事故不致對自然人權利和自由造成「風險」。而在該事故可能對自然人權利和自由造成「高風險」時，方須通知受影響的當事人。

WP29 認為，GDPR 不要求所有侵害皆須通知當事人，是為了保護當事人免受不必要的「通知疲勞」（notification fatigue）。另依 WP29 之解釋，所謂「知悉」侵害事故，係指控管者已在相當程度上確信發生個人資料侵害事故，但知悉之時點應個案判斷[186]。而控管者有義務採取技術保護與組織措施，以便立即確定個人資料侵害是否發生。而在跨境個資侵害事故之情形，控管者應通報 GDPR 第 55 條規定的主責監管機關（lead supervisory authority）[187]。

依 GDPR 第 33 條第 3 項[188]，控管者向主管機關通報個資侵害事故時，至少應提供如下資訊：(1)個人資料侵

[185] EU, GDPR, §33(1), "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."

[186] WP29, Guidelines on Personal data breach notification under Regulation 2016/679 (6 February 2018) 10-11.

[187] WP29, Guidelines on Personal data breach notification under Regulation 2016/679 (6 February 2018) 17.

[188] EU, GDPR, §33(3), "The notification referred to in paragraph 1 shall at least: (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects."

害之性質，如有可能，應包括相關當事人之類別和大致數量，以及相關個人資料紀錄之類別和大致數量；(2)個資保護官之姓名和聯繫方式，或其他聯絡窗口資訊；(3)侵害事故之可能後果；(4)控管者採取或預計採取之侵害因應措施的描述，適當情形下，包括為減輕可能之不利影響而採取之措施。此外，依第 33 條第 1 項，若控管者未於 72 小時時限內通報，還應於通報時說明遲延之理由。

GDPR 第 33 條第 4 項允許分階段通報侵害事故相關資訊，亦即，在無法同時提供資訊之範圍內，可分階段提供資訊，不得有進一步之無故遲延[189]。據此，GDPR 肯認控管者在知悉侵害後 72 小時內無法掌握侵害事故所有必要資訊的可能性。WP29 建議，控管者若要採取分階段通報，應同時告知監管機關將於日後提供更多詳細資訊[190]。

依 GDPR 第 33 條第 2 項[191]，受控管者委託處理個人資料之受託處理者在知悉侵害事故後，應通知控管者，不得無故遲延。該項並未明文規定受託處理者通知控管者之時限，而 WP29 建議受託處理者儘速通知控管者。此外，WP29 亦說明，控管者得與受託處理者訂定契約，約定發生個人資料侵害事故時，由受託處理者通報主管機關及通知當事人，但通知及通報的法律責任仍由控管者承擔[192]。

[189] EU, GDPR, §33(4), "Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay."
[190] WP29, Guidelines on Personal data breach notification under Regulation 2016/679 (6 February 2018) 15.
[191] EU, GDPR, §33(2), "The processor shall notify the controller without undue delay after becoming aware of a personal data breach."
[192] WP29, Guidelines on Personal data breach notification under Regulation 2016/679 (6 February 2018) 14.

依 GDPR 第 33 條第 5 項[193]，控管者應記錄一切個人資料侵害事故，包括與侵害事故相關之事實、影響及已採取之救濟措施。該紀錄應使監管機關得以確認是否遵守第 33 條之規範。WP29 說明，無論侵害是否需要通報監管機關，控管者必須留存所有侵害事故之紀錄[194]。

綜上所述，歐盟 GDPR 要求個資侵害事故原則皆應通報主管機關，且對於通報有嚴格時限。在個資侵害事故可能導致自然人權利和自由之高風險時，應通知個資當事人，且存在法定例外。

（二）美國加州

1、通知當事人

加州 CCPA 並無關於個資侵害事故之規範。但依加州民法典（Civil Code）第 1798.82 條，業者及其他人員有義務就特定個人資訊安全侵害事故進行通知。先予敘明者，相較於 CCPA，民法典（Civil Code）第 1798.82 條第 h 項關於「個人資訊」之定義較窄[195]，僅包括：(1)當事人姓名與其他要素之結合（例如，社會安全碼、駕照

[193] EU, GDPR, §33(5), "The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."

[194] WP29, Guidelines on Personal data breach notification under Regulation 2016/679 (6 February 2018) 26-27.

[195] California, Civil Code, §1798.82(h), "For purposes of this section, "personal information" means either of the following: (1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) Social security number. (B) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual. (C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (D) Medical information. (E) Health insurance information. (F) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes. (G) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5. (2) A username or email address, in combination with a password or security question and answer that would permit access to an online account."

號碼、納稅識別號碼、醫療資訊等）；以及(2)使用者帳號名稱或 Email，結合密碼或足以實現帳號訪問的安全提問與回答。但聯邦、州或地方政府紀錄中依法向一般民眾公開之資訊，不構成個人資訊。因此，業者及其他人員負有侵害通知義務之資訊範圍相對限縮。

依同法第 1798.82 條第 a 項[196]，在加州從事業務之人員或業者，若其擁有或經授權使用的已電腦化的資料包括個人資訊，則應在知悉或被通知資料安全侵害事故後，將該安全事故通知符合下列條件之加州居民：(1)該居民之個人資訊未被加密，且可合理確信其個人資訊已被未經授權之人取得；或(2)該居民之個人資訊已被加密，可合理確信其個人資訊及加密密鑰或安全密碼已被未經授權之人取得，且擁有或經授權使用該加密資訊之人員或業者合理確信，該加密密鑰或安全密碼將使該個人資訊轉為可讀或可使用狀態。

對當事人之通知應儘速進行，不得無故遲延，同時應考量執法機關進行刑事調查之正當需求，以及確定侵害事故範圍及恢復資料系統完整性的必要措施。依同條第 c 項[197]，若執法機關認為通知當事人將妨礙刑事調查，

[196] California, Civil Code, §1798.82(a), "A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."

[197] California, Civil Code, §1798.82(c), "The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation."

得延後通知當事人。執法機關認為通知不會妨礙刑事調查後，應迅速通知當事人。

此外，依第 1798.82 條第 b 項[198]，代他人維持已電腦化的個人資訊之人員或業者，在知悉或合理確信個人資訊已被未經授權之人取得後，應立即通知該個人資訊之所有人或被授權人。

同法第 1798.82 條第 d 項規定了通知之格式並提供通知書例稿。依同條第 j 項[199]，通知得採書面或電子簽章通知方式。於人員或業者可證明存在下列情形之一時，得採取替代通知方式：(1)通知之成本將超過 25 萬美元；(2)受影響之個人超過 50 萬人；(3)該人員或業者並無充分聯絡資訊。替代通知之方式包括 Email 通知、網站顯著位置公告、透過州內主要媒體通知等。

通知應使用簡單易懂的語言，並至少應包含如下資訊：(1)發出通知者的姓名（名稱）和聯絡方式；(2)受侵害的個人資訊類別；(3)發出通知之日期，以及（在可確定相關資訊之前提下）侵害事故的發生日期或推斷發生日期；(4)（在可確定相關資訊之前提下）是否因執法機關調查而延後通知；(5)（在可確定相關資訊之前提下）

[198] California, Civil Code, §1798.82(b), "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

[199] California, Civil Code, §1798.82 (j), "For purposes of this section, "notice" may be provided by one of the following methods: … (3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following: (A) Email notice when the person or business has an email address for the subject persons. (B) Conspicuous posting, for a minimum of 30 days, of the notice on the internet website page of the person or business, if the person or business maintains one. For purposes of this subparagraph, conspicuous posting on the person's or business' internet website means providing a link to the notice on the home page or first significant page after entering the internet website that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link. (C) Notification to major statewide media."

侵害事故之一般描述；(6)（若受影響之資訊包含社會安全碼、駕照號碼或加州身分證號碼）主要信用報告機構的免付費電話和地址；(7)（若發出通知者是侵害事故來源，受影響之資訊包含社會安全碼、駕照號碼、加州身分證號碼等政府頒發之獨特性身分識別號碼）免費協助受影響之個人防範身分竊盜之相關資訊[200]。

2、通報主管機關

依加州民法典（Civil Code）第 1798.82 條第 f 項[201]，若人員或業者就單一侵害事故，依該法需通知之加州居民數目超過 500 人，則應將不含個人資訊之侵害事故通知樣稿以電子方式提交予州檢察長。加州州檢察長在其官方網站上提供資料安全侵害通知搜尋功能[202]，民眾得依據業者名稱或侵害發生日期搜尋侵害通知。

由前開規定可知，美國加州法律中關於個資侵害事故通知之規範與 CCPA 並非精準配合。個資侵害事故通知制度之

[200] California, Civil Code, §1798.82(d)(2), "The security breach notification described in paragraph (1) shall include, at a minimum, the following information: (A) The name and contact information of the reporting person or business subject to this section. (B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach. (C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice. (D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided. (E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided. (F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number. (G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h)."

[201] California, Civil Code, §1798.82(f), "A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code."

[202] California Attorney General, Search Data Security Breaches, https://oag.ca.gov/privacy/databreach/list.

適用對象限於加州居民之身分相關資料和網路服務帳號資料，其制度設立初衷帶有濃厚的防範身分竊盜、維護網路服務帳號安全的色彩。因此，加州的個資侵害事故通知制度著重於對當事人之通知，凡符合條件之侵害事故皆應通知當事人。而只有受影響的個人數目達相當規模時，才要求通知主管機關。

（三）美國維吉尼亞州

1、通知當事人

維吉尼亞州 CDPA 並無關於個資侵害事故通知之規範，但依維吉尼亞州法典（Code of Virginia）第 18.2-186.6 條，個人及實體有義務就特定個人資訊安全侵害事故進行通知。相較於 CDPA，維吉尼亞州法典第 18.2-186.6 條第 A 項關於「個人資訊」之定義相當狹窄[203]，僅包括當事人姓名結合其他要素之結合（例如，社會安全碼、駕照號碼、州身分證號碼、護照號碼、軍人身分證號碼、金融帳號資訊等），且該結合要素以未經加密且未經遮罩內容（redact）者為限。該法另對「遮罩內容」之程度訂有要求。

第 18.2-186.6 條第 B 項規範非加密資訊之侵害事故通知[204]。若個人或實體（entity）擁有或經授權使用的電腦

[203] Virginia, Code of Virginia, § 18.2-186.6(A), “"Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted: 1. Social security number; 2. Driver's license number or state identification card number issued in lieu of a driver's license number; 3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts; 4. Passport number; or 5. Military identification number. The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public….”

[204] Virginia, Code of Virginia, § 18.2-186.6(B), “If unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the individual or entity reasonably believes has caused or will cause, identity theft or another fraud to any resident of the Commonwealth, an individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to the Office of the Attorney

化資料包含個人資訊，可合理確信未經加密或未經遮罩內容的個人資訊被未經授權之人存取並取得，且對本州居民造成（或該個人或實體合理確信已造成或將造成）身分竊盜或其他詐欺，則該個人或實體應於知悉或經通知安全侵害事故後，應通知州檢察長辦公室及所有受影響之本州居民，不得無故遲延。考量該個人或實體查明侵害事故範圍及恢復系統完整性之需求，得合理延後通知。若執法機關認為通知將妨礙民刑事調查或危害國土或國家安全，得延後通知。在執法機關判定通知將不再有妨礙調查或危害安全後，應辦理通知，不得無故遲延。

同條第 C 項規範加密資訊之侵害事故通知[205]。若發生(1)加密資訊以未加密形式被未經授權之人存取並取得，或(2)侵害事故之參與者有權存取加密密鑰且該個人或實體合理確信該事故已造成或將造成對本州居民之身分竊盜或其他詐欺，則應就該侵害事故為通知。

此外，依同條第 D 項，代他人維持已電腦化的個人資訊之人員或實體，在知悉或合理確信個人資訊已被未經授權之人存取並取得後，應通知該個人資訊之所有人或被授權人，不得無故遲延。

第 18.2-186.6 條第 A 項也定義了通知之方式與內容。通知得以書面、電話或電子方式通知。於個人或實體能夠證明存在下列情形之一時，得採取替代通知方式：(1)

General and any affected resident of the Commonwealth without unreasonable delay. Notice required by this section may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system. Notice required by this section may be delayed if, after the individual or entity notifies a law-enforcement agency, the law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security."

[205] Virginia, Code of Virginia, § 18.2-186.6(C), "An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth."

通知之成本將超過 5 萬美元；(2)待通知之受影響本州居民超過 10 萬人；(3)該人員或實體並無充分聯絡資訊。替代通知之方式包括Email通知、網站顯著位置公告、透過州內主要媒體通知等[206]。

通知應包括如下內容[207]：(1)對該事故之一般性描述；(2)受影響個人資訊之類別；(3)該個人或實體防範後續事故之一般性措施；(4)受影響之當事人得尋求更多資訊與協助的聯絡電話（若有）；(5)請受影響之當事人留意銀行對帳單和免費信用報告之建議。

2、 通報主管機關

對於非加密資訊之侵害事故，維吉尼亞州法典第18.2-186.6條第B項要求個人或實體在通知受影響的當事人時，一併通報州檢察長辦公室。

依同條第 E 項[208]，若個人或實體依該條規範需同時通知 1000 人或以上，該個人或實體亦應將侵害事故通知之時點、方式和內容通報州檢察長辦公室和全國性消費者報告機構。

---

[206] Virginia, Code of Virginia, § 18.2-186.6(A), "…"Notice" means: 1. Written notice to the last known postal address in the records of the individual or entity; 2. Telephone notice; 3. Electronic notice; or 4. Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or consent to provide notice as described in subdivisions 1, 2, or 3 of this definition. Substitute notice consists of all of the following: a. E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents; b. Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and c. Notice to major statewide media...."

[207] Virginia, Code of Virginia, § 18.2-186.6(A), "…Notice required by this section shall include a description of the following: (1) The incident in general terms; (2) The type of personal information that was subject to the unauthorized access and acquisition; (3) The general acts of the individual or entity to protect the personal information from further unauthorized access; (4) A telephone number that the person may call for further information and assistance, if one exists; and (5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports…."

[208] Virginia, Code of Virginia, § 18.2-186.6(E), "In the event an individual or entity provides notice to more than 1,000 persons at one time pursuant to this section, the individual or entity shall notify, without unreasonable delay, the Office of the Attorney General and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a (p), of the timing, distribution, and content of the notice."

此外，對於涉及納稅人識別號碼之薪資稅費扣繳資訊侵害事故，同條第 M 項要求僱主或薪資委外服務者向州檢察長辦公室通報。

由前開規定可知，美國維吉尼亞州的個資侵害事故通知制度與加州整體架構相似，但細部內容不同。兩州制度皆以防範身分詐欺為主要目的，皆以資料所有人或被授權人為通知與通報義務人，並規範代為維持資料人向所有人或被授權人之通知義務。兩者關於延後通報之規範也相當類似。

兩州制度主要區別如下：首先，加州侵害事故通知制度適用於身分資訊和網路服務帳號資訊，而維吉尼亞州制度所適用的個人資訊範圍比加州更為限縮，僅適用於身分資訊。

其次，加州對各類個人資訊之侵害事故適用同等通知與通報制度，維吉尼亞州則因所涉個人資訊性質不同，而有不同要求。維吉尼亞州對於非加密個人資訊，如發生法定侵害事故，即需在通知當事人時一併通報州檢察長，且。對於加密資訊，則在法定侵害事故所涉人數達一定規模時，方需通報報州檢察長及消費者報告機構。又因維吉尼亞州所定義之個人資訊不包含納稅人識別號碼，故在一般通知與通報義務之外，尚有關於員工或受薪者薪資稅費扣繳資訊侵害事故通報之特別規範。

第三，加州對於發生侵害事故的資料所有人或被授權人義務要求更為嚴格。依加州制度，有侵害發生之事實時，所有人或被授權人原則即應通知當事人和通報州檢察長。而維吉尼亞州制度則容許資料所有人或被授權人判斷對州內居民之危害風險，再據此決定是否通知或通報。

（四）日本個人資訊保護法

1、通知當事人

日本於 2020 年 6 月修正個人資訊保護法前，日本個人資訊保護委員會透過「平成 29（2017）年個人資訊保護委員會第１号通知」[209]，訂定個人資料外洩等侵害事故因應措施，其中包含為防範後續侵害[210]、防止類似事故發生等目的，聯絡受影響之個人，以及向個人資訊保護委員會通報。

依 2020 年 6 月修正後之個人資訊保護法，個人資訊處理事業須將符合條件之個人資料外洩、滅失、毀損等安全侵害事故通報主管機關並通知受影響之當事人，由此從法律層面確立個人資料侵害事故之通知與通報制度。

依日本個人資訊保護法第 22-2 條[211]，個人資訊處理事業所處理之個人資料如發生外洩、滅失、毀損或其他安全事故，且因此存在個人資訊保護委員會所定規則中規範之個人權利和利益侵害之高風險，則個人資訊處理事業應依個人資訊保護委員會規則，通知個資當事人。同條第 2 項但書規定，於難以通知個資當事人，且個人資訊處理事業為保護個資當事人權利和利益採取必要替代措施者，不適用前開通知規範。

關於負有通知義務的個人資訊處理事業範圍，日本個人資訊保護法第 22-2 條第 1 項規定，若個人資訊處理

---

[209] 個人データの漏えい等の事案が発生した場合等の対応について（平成 29 年個人情報保護委員会告示第１号），https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf。

[210]「後續侵害」原文為「二次被害」，意指因侵害事故未獲有效因應而延伸出的進一步侵害。

[211] 日本，個人情報保護法，§22-2，「１　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を個人情報保護委員会に報告しなければならない。ただし、当該個人情報取扱事業者が、他の個人情報取扱事業者から当該個人データの取扱いの全部又は一部の委託を受けた場合であって、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を当該他の個人情報取扱事業者に通知したときは、この限りでない。２　前項に規定する場合には、個人情報取扱事業者（同項ただし書の規定による通知をした者を除く。）は、本人に対し、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を通知しなければならない。ただし、本人への通知が困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。」。

事業受其他個人資訊處理事業委託處理所涉個人資料之全部或一部時，應依個人資訊保護委員會規則通知該其他個人資訊處理事業，而不適用當事人通知義務。

依個人資訊保護委員會訂定之日本個人資訊保護法施行規則第 6-2 條[212]，已發生或可能發生下列個人資料之外洩、滅失或毀損（以下稱「外洩等」）事故之一時，存在「個人權利和利益侵害之高風險」：(1)該個人資料包含敏感個人資訊；(2)可能因不法利用而導致財產損害；(3)個人資料外洩可能基於不法目的；或(4)所涉個資當事人數目超過 1000 人。但是，若個人資訊處理事業已採行複雜加密措施或其他保護當事人權利和利益之必要措施，則不存在前述個人權利和利益侵害之高風險。

個人資訊保護法施行規則第 6-5 條係通知當事人之規範[213]。依該規定，個人資訊處理事業知悉同規則第 6-2 條所列應予通知之情形後，應在保護當事人權利和利益之必要範圍內，儘速通知當事人如下事項：(1)事故概況；(2)所涉個人資料之類別；(3)外洩等事故之發生原因；(4)是否存在後續侵害及其內容；(5)其他相關事項。依同規則第 6-3 條，通知之具體內容，以作出通知時個人資訊處理事業所知者為限。

---

[212] 日本，個人情報の保護に関する法律施行規則，§6-2，「法第二十二条の二第一項本文の個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものは、次の各号のいずれかに該当するものとする。一　要配慮個人情報が含まれる個人データ（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下この条及び次条第一項において同じ。）の漏えい、滅失若しくは毀損（以下「漏えい等」という。）が発生し、又は発生したおそれがある事態。二　不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態。三　不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態。四　個人データに係る本人の数が千人を超える漏えい等が発生し、又は発生したおそれがある事態。」。

[213] 日本，個人情報の保護に関する法律施行規則，§6-5，「個人情報取扱事業者は、法第二十二条の二第二項本文の規定による通知をする場合には、第六条の二各号に定める事態を知った後、当該事態の状況に応じて速やかに、当該本人の権利利益を保護するために必要な範囲において、第六条の三第一項第一号、第二号、第四号、第五号及び第九号に定める事項を通知しなければならない。」。

關於日本個人資訊保護法第 22-2 條第 2 項但書所稱因「難以通知個資當事人」而採取「必要替代措施」之適用，日本個人資訊保護委員會於 2021 年 8 月修正個人資訊保護法指引（個人情報の保護に関する法律についてのガイドライン）（通則編），提供例示說明。若保有之個人資料不含當事人之聯絡方式，或因聯絡資訊過於陳舊，而於通知時無法聯絡到當事人，均屬「難以通知」之情事。而得採行的替代措施，則應包括公告該侵害事故，或設置聯絡窗口以供當事人確認自身資料是否遭侵害等。該指引並說明，作為替代措施之公告內容雖應依個案確定，但應以當事人通知事項為基礎。此外，縱使不以公告為替代措施，從防範後續侵害、防止類似事故再次發生之角度，宜根據個案情形而予以公告[214]。

此外，依日本個人資訊保護法第 35-2 條第 9 項[215]，假名資訊、構成假名資料之個人資料以及構成假名資料之保有個人資料，不適用第 22-2 條所規定個資侵害事故通知與通報制度。因此，前述規範，以及下文所述通報主管機關相關規範，不適用經假名化處理之個人資料。

2、 通報主管機關

依日本個人資訊保護法第 22-2 條第 1 項[216]，個人資訊處理事業向個人資訊保護委員會通報個人資料外洩等

[214] 日本，個人情報保護委員会，平成 28 年 11 月（令和 3 年 8 月一部改正），個人情報の保護に関する法律についてのガイドライン（通則編），第 60-61 頁。

[215] 日本，個人情報保護法，§35-2(9)，「仮名加工情報、仮名加工情報である個人データ及び仮名加工情報である保有個人データについては、第十五条第二項、第二十二条の二及び第二十七条から第三十四条までの規定は、適用しない。」。

[216] 日本，個人情報保護法，§22-2(1)，「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を個人情報保護委員会に報告しなければならない。ただし、当該個人情報取扱事業者が、他の個人情報取扱事業者から当該個人データの取扱いの全部又は一部の委託を受けた場合であって、個人情報

事故之條件，與通知個資當事人之條件基本相同。概言之，如發生個人資料外洩等事故，且存在個人權利和利益侵害之高風險，則個人資訊處理事業應依個人資訊保護委員會規則，通報個人資訊保護委員會。「個人權利和利益侵害之高風險」之判定依據，係前述個人資訊保護法施行規則第 6-2 條。

個人資訊保護法施行規則第 6-3 條係通報主管機關之規範。個人資訊處理事業知悉同規則第 6-2 條所列應予通知之情形後，應儘速向個人資訊保護委員會通報下列事項：(1)事故概況；(2)所涉個人資料之類別；(3)所涉個資當事人數目；(4)外洩等事故之發生原因；(5)是否存在後續侵害及其內容；(6)向當事人通知之狀況；(7)事故之公開情形；(8)防範事故再次發生之措施；(9)其他相關事項。通報之具體內容，以進行通報時個人資訊處理事業所知者為限[217]。

關於向主管機關通報之時限，依個人資訊保護法施行規則第 6-3 條第 2 項[218]，因不法目的所致個人資料外洩等事故應於知悉後 60 日內通報，其他事故應於知悉後 30 日內通報。

於受託處理個人資料之情形，受託之個人資訊處理事業應依個人資訊保護委員會所定規則，通知委託之個

保護委員会規則で定めるところにより、当該事態が生じた旨を当該他の個人情報取扱事業者に通知したときは、この限りでない。」。

[217] 日本，個人情報の保護に関する法律施行規則，§6-3(1)，「個人情報取扱事業者は、法第二十二条の二第一項本文の規定による報告をする場合には、前条各号に定める事態を知った後、速やかに、当該事態に関する次に掲げる事項（報告をしようとする時点において把握しているものに限る。次条において同じ。）を報告しなければならない。一　概要。二　漏えい等が発生し、又は発生したおそれがある個人データの項目。三　漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数。四　原因。五　二次被害又はそのおそれの有無及びその内容。六　本人への対応の実施状況。七　公表の実施状況。八　再発防止のための措置。九　その他参考となる事項。」。

[218] 日本，個人情報の保護に関する法律施行規則，§6-3(2)，「前項の場合において、個人情報取扱事業者は、当該事態を知った日から三十日以内（当該事態が前条第三号に定めるものである場合にあっては、六十日以内）に、当該事態に関する前項各号に定める事項を報告しなければならない。」。

人資訊處理事業，而無需通報個人資訊保護委員會或個資當事人。依個人資訊保護法施行規則第 6-4 條[219]，受託個人資訊處理事業知悉同規則第 6-2 條所列應予通知之情形後，應儘速通知委託個人資訊處理事業，通知內容與第 6-3 條所列向個人資訊保護委員會之通報事項相同。

由前開規範可知，依日本個人資訊保護法，個人資料外洩等事故向當事人通知與向主管機關通報之條件基本相同，且其核心判斷要件為對當事人權利和利益之「高風險」。若個人資訊處理事業已採取複雜加密或其他必要措施，能夠在外洩等事故發生後，保護當事人權利和利益，則認為不存在高風險。於該法配合數位社會整備法修正後，前開規範雖有條號及文字調整，但其內容並無實質變化。

（五）日本行政機關適用新法

現行日本行政機關個人資訊保護法並未規定個人資訊外洩通知制度。但依日本行政程序中識別性個人編號使用法（以下稱個人編號使用法）[220]第 29-4 條[221]，若發生「特定個人資訊」外洩或其他影響特定個人資訊安全之重大事件，個人編號利用事務實施者應向日本個人資訊保護委員會通報。

依同法第 2 條之定義，所謂「特定個人資訊」，係指包含個人編號之個人資訊[222]；所謂個人資訊，係指行政機關個

[219] 日本，個人情報の保護に関する法律施行規則，§6-4，「個人情報取扱事業者は、法第二十二条の二第一項ただし書の規定による通知をする場合には、第六条の二各号に定める事態を知った後、速やかに、前条第一項各号に定める事項を通知しなければならない。」。

[220] 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成二十五年法律第二十七号，令和三年法律第十一号による改正，以下「番号利用法」という）。

[221] 日本，番号利用法，§29-4，「個人番号利用事務等実施者は、個人情報保護委員会規則で定めるところにより、特定個人情報ファイルに記録された特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態が生じたときは、委員会に報告するものとする。」。

[222] 日本，番号利用法，§2(6)，「この法律において「特定個人情報」とは、個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。第七条第一項及び第二項、第八条並びに第四十八条並びに附

人資訊保護法所定義之個人資訊；所謂「個人編號」，係指由日本住民票號碼變換而得、可識別該住民票持有者之編號[223]；所謂「個人編號利用事務」，係指行政機關、地方公共團體、獨立行政法人及其他行政事務處理者，依該法規定之個人編號利用規範，在高效檢索及管理個人編號之必要範圍內，對個人編號之利用與處理事務[224]。據此，日本行政機關等個人編號利用事務實施者，若發生特定個人資訊外洩等重大安全事故，應通報主管機關。

如前所述，日本國會於 2021 年 5 月通過數位社會整備法，將行政機關亦納入個人資訊保護法之適用範圍。經數位社會整備法修正的個人資訊保護法將新增行政機關之個人資料外洩通知與通報義務，詳述如下。

1、 通知當事人

依數位社會整備法修正後個人資訊保護法第 68 條[225]，若保有個人資訊如發生外洩、滅失、毀損或其他安全事

則第三条第一項から第三項まで及び第五項を除き、以下同じ。）をその内容に含む個人情報をいう。」。

223 日本，番号利用法，§2(5)，「この法律において「個人番号」とは、第七条第一項又は第二項の規定により、住民票コード（住民基本台帳法（昭和四十二年法律第八十一号）第七条第十三号に規定する住民票コードをいう。以下同じ。）を変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう。」。

224 日本，番号利用法，§2(10)，「この法律において「個人番号利用事務」とは、行政機関、地方公共団体、独立行政法人等その他の行政事務を処理する者が第九条第一項又は第二項の規定によりその保有する特定個人情報ファイルにおいて個人情報を効率的に検索し、及び管理するために必要な限度で個人番号を利用して処理する事務をいう。」。

225 日本，個人情報の保護に関する法律（平成十五年法律第五十七号，令和三年法律第三十七号による改正，以下「新個人情報保護法」という），§68，「1　行政機関の長等は、保有個人情報の漏えい、滅失、毀損その他の保有個人情報の安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を個人情報保護委員会に報告しなければならない。2　前項に規定する場合には、行政機関の長等は、本人に対し、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を通知しなければならない。ただし、次の各号のいずれかに該当するときは、この限りでない。一　本人への通知が困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるとき。二　当該保有個人情報に第七十八条各号に掲げる情報のいずれかが含まれるとき。」。

故，且因此存在個人資訊保護委員會規則所規範之個人權利和利益侵害之高風險，則行政機關首長應依個人資訊保護委員會規則，通知個資當事人，但有下列情形之一者，不在此限：(1)難以通知個資當事人，且已採取必要替代措施保護個資當事人權利和利益；(2)所涉保有個人資訊包含修正後個人資訊保護法第 78 條（對應現行行政機關個人資訊保護法第 14 條）所列不予揭露之個人資訊。

2、通報主管機關

依數位社會整備法修正後個人資訊保護法第 68 條第 1 項，行政機關首長向個人資訊保護委員會通報保有個人資訊外洩等事故之條件，與通知個資當事人之條件基本相同。概言之，如發生保有個人資訊外洩等事故，且存在個人權利和利益侵害之高風險，則行政機關首長應依個人資訊保護委員會規則，通報個人資訊保護委員會。

綜上所述，日本現行法規中，僅包含特定個人資訊之外洩通報制度。於配合數位社會整備法修正後，日本將引入行政機關保有個人資訊外洩等事故通知與通報制度。

（六）韓國個人資料保護法

1、通知當事人

韓國個人資料保護法第 34 條係關於個人資料外洩通知/通報制度之規範。依該條第 1 項，個人資料處理者知悉個人資料外洩後，應儘速將下列事項告知當事人：(1)外洩個人資料之類別；(2)外洩之發生時間與經過；(3)個資當事人可採取何種措施降低外洩所致風險；(4)個人資料處理者所採取的因應措施和救濟程序；(5)個資當事人

受有損害時，可受理損害申訴之部門及聯絡方式。依同法第 34 條第 2 項，個人資料處理者應置備因應措施並採取相應對策，以將外洩所致損害最小化[226]。

個人資料保護法施行令第 40 條規定了通知當事人之時點和方法[227]。依該條規定，個人資料處理者應於知悉外洩事故後，儘速以書面通知受影響之當事人，但若個人資料處理者需要採取緊急因應措施防範外洩資料傳播或外洩進一步擴大，得於採取該等措施後儘速書面通知當事人。

若個人資料處理者在知悉外洩事故或採取緊急因應措施後，尚未掌握個人資料保護法第 34 條第 1 項所列法定應通知之所有事項，得先行通知已發生外洩及所涉個人資料，其餘內容後續補充通知。若受影響之個資當事

---

[226] 한국，개인정보보호법，§34，“① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다. 1. 유출된 개인정보의 항목. 2. 유출된 시점과 그 경위. 3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보. 4. 개인정보처리자의 대응조치 및 피해 구제절차. 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처. ② 개인정보처리자는 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.…”

[227] 한국，개인정보보호법시행령，§40，“① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 서면등의 방법으로 지체 없이 법 제 34 조제 1 항 각 호의 사항을 정보주체에게 알려야 한다. 다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검・보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 지체 없이 정보주체에게 알릴 수 있다. ② 제 1 항에도 불구하고 개인정보처리자는 같은 항 본문에 따라 개인정보가 유출되었음을 알게 되었을 때나 같은 항 단서에 따라 유출 사실을 알고 긴급한 조치를 한 후에도 법 제 34 조제 1 항제 1 호 및 제 2 호의 구체적인 유출 내용을 확인하지 못한 경우에는 먼저 개인정보가 유출된 사실과 유출이 확인된 사항만을 서면등의 방법으로 먼저 알리고 나중에 확인되는 사항을 추가로 알릴 수 있다.③ 제 1 항과 제 2 항에도 불구하고 법 제 34 조제 3 항 및 이 영 제 39 조제 1 항에 따라 1 천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 법 제 34 조제 1 항 각 호의 사항을 7 일 이상 게재하여야 한다. 다만, 인터넷 홈페이지를 운영하지 아니하는 개인정보처리자의 경우에는 서면등의 방법과 함께 사업장등의 보기 쉬운 장소에 법 제 34 조제 1 항 각 호의 사항을 7 일 이상 게시하여야 한다.“

人數目達 1000 人，個人資料處理者除書面通知各當事人外，還應將法定通知事項於其網站公告至少 7 日；個人資料處理者如無網站，則應在書面通知當事人的同時，將法定通知事項公告於其工作場所顯著位置至少 7 日。

對於資訊與通訊服務提供者，韓國個人資料保護法第 39-4 條個資外洩通知之特殊規範。依該條第 1 項[228]，資訊與通訊服務提供者（含其依法分享或揭露使用者資料之第三人）若發生使用者資料滅失、竊盜或外洩（合稱「外洩等」），原則應於知悉後 24 小時內通知相關使用者，通知內容與第 34 條第 1 項所列法定通知事項相同。如因正當理由無法於期限內通知（例如，不知使用者聯絡資訊），則可依個人資料保護法施行令採取替代措施。

依個人資料保護法施行令第 48-4 條[229]，因正當理由無法於期限內通知當事人時，資訊與通訊服務提供者得

---

228 한국，개인정보보호법，§39-4(1)，“제 34 조제 1 항 및 제 3 항에도 불구하고 정보통신서비스 제공자와 그로 부터 제 17 조제 1 항에 따라 이용자의 개인정보를 제공받은 자(이하 "정보통신서비스 제공자등"이라 한다)는 개인정보의 분실・도난・유출(이 하 "유출등"이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 사항 을 해당 이용자에게 알리고 보호위원회 또는 대통령령으로 정하는 전 문기관에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24 시간을 경과하여 통지・신고해서는 아니 된다. 다만, 이용자의 연락처 를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.”

229 한국 ，개인정보보호법시행령 ，§48-4 ，“…② 정보통신서비스 제공자등은 개인정보의 분실・도난・유출의 사실을 안 때에는 지체 없이 법 제 39 조의 4 제 1 항 각 호의 모든 사항을 서면등의 방법으로 이용자에게 알리고 보호위원회 또는 한국인터넷진흥원에 신고해야 한다. ③ 정보통신서비스 제공자등은 제 2 항에 따른 통지・신고를 하려는 경우에는 법 제 39 조의 4 제 1 항제 1 호 또는 제 2 호의 사항에 관한 구체적인 내용이 확인되지 않았으면 그때까지 확인된 내용과 같은 항 제 3 호부터 제 5 호까지의 사항을 우선 통지・신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지・신고해야 한다.④ 정보통신서비스 제공자등은 법 제 39 조의 4 제 1 항 각 호 외의 부분 단서에 따른 정당한 사유가 있는 경우에는 법 제 39 조의 4 제 1 항 각 호의 사항을 자신의 인터넷 홈페이지에 30 일 이상 게시하는 것으로 제 2 항의 통지를 갈음할 수 있다.⑤ 천재지변이나 그 밖의 부득이한 사유로 제 4 항에 따른 홈페이지 게시가 곤란한 경우에는 「 신문 등의 진흥에 관한 법률 」에 따른 전국을

將法定通知事項公告於其網站，公告期間至少應達 30 日。若因不可抗力或其他類似原因，無法在資訊與通訊服務提供者網站上公告，則應將公告內容在至少兩家全國性綜合日報上刊載至少一次。

韓國個人資料保護法第 28-7 條包含對假名資料之特殊規定[230]。依該條，同法第 34 條第 1 項及第 39-4 條不適用於假名資料。因此，若發生假名資料外洩事故，個人資料處理者不負外洩通知義務，但仍應依 34 條第 2 項準備因應措施並採取相應對策，以求將外洩所致損害最小化。

2、 通報主管機關

韓國個人資料保護法第 34 條第 3 項規定[231]，若外洩之個人資料達個人資料保護法施行令所定規模，個人資料處理者應儘速將下列資訊通報予個人資料保護委員會或個人資料保護法施行令指定之專門機關：(1)依同法第 34 條第 1 項進行通知之狀況，以及(2)依同法第 34 條第 2 項採取必要措施之結果。個人資料保護委員會或該專門機構得為防範損害擴大及補救損害而提供技術支援。

보급지역으로 하는 둘 이상의 일반일간신문에 1 회 이상 공고하는 것으로 제 4 항에 따른 홈페이지 게시를 갈음할 수 있다.…”

[230] 한국，개인정보보호법，§28-7，“가명정보는 제 20 조, 제 21 조, 제 27 조, 제 34 조제 1 항, 제 35 조부터 제 37 조까지, 제 39 조의 3, 제 39 조의 4, 제 39 조의 6 부터 제 39 조의 8 까지의 규정을 적용하지 아니한다.”

[231] 한국 ，개인정보보호법 ，§34(3) ，“개인정보처리자는 대통령령으로 정한 규모 이상의 개인정보가 유출된 경우에는 제 1 항에 따른 통지 및 제 2 항에 따른 조치 결과를 지체 없이 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 보호위원회 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 154 등을 위한 기술을 지원할 수 있다.”

依個人資料保護法施行令第 39 條第 1 項[232]，所謂「規模以上之個人資料外洩事故」係指受影響之個資當事人達 1000 人之外洩事故。

對於資訊與通訊服務提供者，韓國個人資料保護法第 39-4 條第 1 項要求，資訊與通訊服務提供者若發生使用者資料滅失、竊盜或外洩（合稱「外洩等」），應於知悉後 24 小時內通報主管機關。如存在無法於 24 小時內通知之正當理由，應向個人資料保護委員會說明。依個人資料保護法施行令第 48-4 條，該等正當理由應儘速以書面向個人資料保護委員會說明。

由前開規範可知，韓國個人資料保護法要求一切個資外洩皆通知受影響的當事人，而外洩達一定規模（所涉當事人達 1000 人）時，則應通報主管機關。資訊與通訊服務提供者之使用者個資外通知義務則更為嚴格，應通報之事故範圍更廣（除外洩外，尚包括滅失、竊盜之情事），通報時限原則限於知悉後 24 小時內，且任一事故皆應通報主管機關，不適用 1000 人規模要求。此外，或因考量假名資料之識別性較低，韓國之個資外洩通知制度不適用於假名資料。

（七）新加坡個人資料保護法

1、通知當事人

新加坡於 2020 年修訂 PDPA 之前，新加坡個人資料保護委員會（PDPC）發布「資料侵害管理指引」[233]，將通知當事人與通報個人資料保護委員會列為管理個人資料侵害事故之最佳實務做法。

---

[232] 한국，개인정보보호법시행령，§39(1)，“법 제 34 조제 3 항 전단에서 “대통령령으로 정한 규모 이상의 개인정보”란 1 천명 이상의 정보주체에 관한 개인정보를 말한다.”

[233] Singapore PDPC, Guide to Managing Data Breaches (8 May 2015).

2019 年，個人資料保護委員會計劃導入強制性個人資料侵害事故通知與通報制度，因此先行修改資料侵害管理指引，以協助組織適應法規變化[234]。2020 年 11 月，新加坡修訂 PDPA，增設第 6A 部分，以第 26A 條至第 26E 條五個條文，正式引入強制性個人資料侵害事故通知與通報制度。

新加坡進而於 2021 年 2 月頒行 2021 年個人資料保護（資料侵害通知）條例（Personal Data Protection (Notification of Data Breaches) Regulations 2021, 以下稱侵害通知條例），新加坡個人資料保護委員會亦於同年 3 月依據新法再行修訂資料侵害管理指引[235]。

依新加坡 PDPA 第 26A 條[236]，資料侵害係指(1)未經授權而存取、蒐集、使用、揭露、複製、修改或處置個人資料，或(2)存有個人資料之媒介或裝置滅失，且可能因此發生個人資料未經授權而被存取、蒐集、使用、揭露、複製、修改或處置。

依新加坡 PDPA 第 26B 條，下列資料侵害構成「應通知之資料侵害」。但於組織內部發生的資料未經授權而被存取、蒐集、使用、揭露、複製或修改，不構成應通知之資料侵害。(1)侵害事故造成或可能造成受影響之個人受到嚴重損害[237]。第 26B 條第 2 項舉例說明[238]，若

[234] Singapore PDPC, Guide to Managing Data Breaches 2.0 (22 May 2019).
[235] Singapore PDPC, Guide on Managing and Notifying Data Breaches Under the PDPA (15 March 2021).
[236] Singapore, PDPA, §26A, "In this Part, unless the context otherwise requires —…"data breach", in relation to personal data, means —(a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or (b) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur."
[237] Singapore, PDPA, §26B(1), "A data breach is a notifiable data breach if the data breach —(a) results in, or is likely to result in, significant harm to an affected individual; or (b) is, or is likely to be, of a significant scale."
[238] Singapore, PDPA, §26B(2), "Without limiting subsection (1)(a), a data breach is deemed to result in significant harm to an individual — (a) if the data breach is in relation to any prescribed personal data or class of personal data relating to the individual; or (b) in other prescribed circumstances."

侵害事故涉及「法定個資」（prescribed personal data）或「法定個資類別」，或有其他法定情事，則視為對個人造成嚴重損害。侵害通知條例對法定個資、法定個資類別和法定情事作出具體規範。

概言之，若侵害涉及當事人之姓名、別名、身分識別號碼、帳號和存取該帳號之密碼或其他驗證資訊、薪資或其他財產資訊、信用卡號、銀行或其他金融機構帳號、特定醫療資訊等。但公開可得（因任何侵害事故而公開者除外）之資訊，或依成文法公開之資訊，不屬於法定個資、法定資料類別或法定情事。(2)侵害具有或可能具有較大規模。第 26B 條第 3 項舉例說明[239]，若侵害事故之影響人數達法定數目，或有其他法定情事，則視為具有較大規模。依侵害通知條例，所謂法定數目係指 500 人。

依新加坡 PDPA 第 26C 條[240]，組織若合理認為其所持有或控制之個人資料發生侵害事故，應儘速對侵害事故執行評估，以判斷該事故是否為「應通知之資料侵害」。若代其他組織處理個人資料之資料中間商（代公共機構處理個人資料者除外）合理認為其代為處理之個人資料發生侵害事故，應儘速通知該其他組織，該其他組織應於收到通知後儘速對侵害事故執行評估。

[239] Singapore, PDPA, §26B(3), "Without limiting subsection (1)(b), a data breach is deemed to be of a significant scale —(a) if the data breach affects not fewer than the prescribed number of affected individuals; or (b) in other prescribed circumstances."

[240] Singapore, PDPA, §26C, "…(2) Subject to subsection (3), where an organisation has reason to believe that a data breach affecting personal data in its possession or under its control has occurred, the organisation must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach…. (3) Where a data intermediary (other than a data intermediary mentioned in section 26E) has reason to believe that a data breach has occurred in relation to personal data that the data intermediary is processing on behalf of and for the purposes of another organisation — (a) the data intermediary must, without undue delay, notify that other organisation of the occurrence of the data breach; and (b) that other organisation must, upon notification by the data intermediary, conduct an assessment of whether the data breach is a notifiable data breach…."

依新加坡 PDPA 第 26D 條第 2 項[241]，組織判定存在應通知之資料侵害後，應在通報個人資料保護委員會的同時、或通報之後，以合理方式通知受影響之個人。依同條第 5 項，下列情形下，組織得不通知受影響的當事人：(1)在評估判定該事故係「應通知之資料侵害」的同時或之後，組織依相關規定採取措施，使侵害事故幾乎不致對受影響之個人造成嚴重損害；或(2)在「應通知之資料侵害」發生前，組織已採取技術措施，使事故幾乎不致對受影響之個人造成嚴重損害。依同條第 6 項[242]，若執法機關或個人資料保護委員會指示不得通知受影響之個人，則組織應遵守此等指示。依同條第 7 項[243]，組織得向個人資料保護委員會提出書面申請，請求豁免當事人通知義務；個人資料保護委員會得視情形批准豁免。

關於通知當事人之內容，依侵害通知條例第 6 條[244]，應包含：(1)組織知悉該侵害事故之經過；(2)所涉個人資

[241] Singapore, PDPA, §26D, "…(2) Subject to subsections (5), (6) and (7), on or after notifying the Commission under subsection (1), the organisation must also notify each affected individual affected by a notifiable data breach mentioned in section 26B(1)(a) in any manner that is reasonable in the circumstances….(5) Subsection (2) does not apply to an organisation in relation to an affected individual if the organisation —(a) on or after assessing that the data breach is a notifiable data breach, takes any action, in accordance with any prescribed requirements, that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual; or (b) had implemented, prior to the occurrence of the notifiable data breach, any technological measure that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual."

[242] Singapore, PDPA, §26D(6), "An organisation must not notify any affected individual in accordance with subsection (2) if — (a) a prescribed law enforcement agency so instructs; or (b) the Commission so directs."

[243] Singapore, PDPA, §26D(7), "The Commission may, on the written application of an organisation, waive the requirement to notify an affected individual under subsection (2) subject to any conditions that the Commission thinks fit."

[244] Singapore, Personal Data Protection (Notification of Data Breaches) Regulations 2021, §6, "For the purposes of section 26D(3) of the Act, the notification by an organisation to an affected individual affected by a notifiable data breach under section 26D(2) of the Act must contain all of the following information: (a) the circumstances in which the organisation first became aware that the notifiable data breach had occurred; (b) the personal data or classes of personal data relating to the affected individual affected by the notifiable data breach; (c) the potential harm to the affected individual as a result of the notifiable data breach; (d) information on any action by the organisation, whether taken before or to be taken after the organisation notifies the affected individual —(i) to eliminate or mitigate any potential harm to the affected individual as a result of the notifiable data breach; and (ii) to address or remedy any failure or shortcoming that the organisation believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach; (e) the steps that the affected individual may take to eliminate or mitigate any potential harm as a result of the notifiable data breach, including preventing the misuse of the affected individual's personal data affected by the notifiable

料之內容或類別；(3)該侵害事故對當事人可能造成之損害；(4)組織在通知前或通知後已採取的消除或減輕可能損害以及處置事故發生原因之措施；(5)當事人為消除或減輕可能損害得採取之措施；以及(6)組織至少一名授權代表之聯絡方式。

關於通知當事人之「合理方式」，新加坡個人資料保護委員會於指引中說明[245]，組織應確保其通知方式能夠適當、有效且及時地聯絡到當事人。組織得使用其與當時人溝通之通常方式，將個資侵害事故通知予當事人。若組織並無與當事人溝通之通常方式，組織應確定最適當的通知方式。由於隨著技術的發展，通知方式也更趨多元，組織得據此確定最高效的通知方式。

2、通報主管機關

依新加坡 PDPA 第 26D 條第 1 項，組織判定存在應通知之資料侵害後，應儘速通報個人資料保護委員會，並至遲應在判定後 3 日內通報。

侵害通知條例第 5 條規定了向主管機關通報的內容與形式。通報應使用個人資料保護委員會網站公布之方式[246]，並應包含以下內容：(1)組織知悉該侵害事故之日期與過程；(2)依時間順序描述組織知悉該侵害事故後所採取的措施，包括對事故是否構成「應通知之資料侵害」之評估；(3)該侵害事故之發生過程；(4)該侵害事故所影響之個人數目；(5)該侵害事故所涉個人資料之內容或類

data breach; (f) the business contact information of at least one authorised representative of the organisation."

[245] Singapore PDPC, Advisory Guidelines on Key Concepts in the PDPA (1 October 2021), paras. 20.35-20.36.

[246] 新加坡個人資料保護委員會設有侵害事故通報專用網頁：https://eservice.pdpc.gov.sg/case/db；且對於重大侵害事故，得於工作時間電話通報。See, Singapore PDPC, Guide on Managing and Notifying Data Breaches Under the PDPA (15 March 2021) 38.

別；(6)該侵害事故對當事人之可能損害；(7)通報前或通報後，組織已採取的消除或減輕可能損害、以及處置事故發生原因的措施；(8)組織在通報之同時或通報後，將該侵害事故及消除或減輕可能損害之方法，通知予全部或部分當事人、或一般民眾之計畫；(9)組織至少一名授權代表之聯絡方式。此外，若組織未能於 3 日期限內通報，還應說明遲延通報之原因並提供相應證據。若組織計劃不通知當事人，應於通報中說明不通知當事人之理由。

依新加坡 PDPA 第 26D 條第 9 項，組織依該條通報主管機關及通知當事人之義務，不影響其他法律規定之個資外洩相關通知、通報或資訊提供義務。

由前開規範可知，依新加坡 PDPA，應通知資料侵害之判定標準核心為對當事人之嚴重損害或侵害具較大規模。應通知資料侵害皆須通報主管機關並通知當事人，但在採取措施防範有效防範對當事人嚴重損害的前提下，得例外不通知當事人。此外，在通知時限與內容方面，通報主管機關之要求都比通知當事人更為嚴格。

四、法規比較

自上述比較法觀察，不同國家之個資侵害通知制度在制度架構、可裁量性、法定例外等方面，可能有較大差異，以下將從三個層面分別比較。

（一）個資侵害通知制度架構

若將通知當事人與通報主管機關視為個資侵害通知與通報制度之兩項支柱，並據此分析個資侵害通知制度架構，可將我國及國外之個資侵害通知制度大致分為以下幾類：

1、通知當事人為主，通報主管機關為輔

個資侵害通知制度之重心在於使當事人瞭解個資遭到外洩或其他侵害之事實，並據此注意防範權益受損。我國、美國加州、美國維尼亞州，以及韓國適用於一般個人資料處理者之個資侵害通知制度皆屬此類。

我國個資法僅要求侵害事故發生機關將符合條件之個資侵害事故通知當事人。將個資侵害事故通報主管機關之要求，散見於各中央目的事業主管機關依個資法訂定之管理辦法，且其在通報範圍、時限、配套措施等方面之規範不盡一致。美國加州個資侵害通知制度目的帶有濃厚的防範身分竊盜、維護網路服務帳號安全的色彩。業者在同一侵害事故影響人數達一定規模時，須將當事人通知樣稿提交予州檢察長，由州檢察長公布於專門網頁。因此，加州制度下，主管機關更多地承擔備案功能，而非對個資侵害事故施以主動監管。美國維吉尼亞州個資侵害通知制度之整體架構則與美國加州相似，前文已有分析。

較之於我國和加州，韓國適用於一般個人資料處理者之個資侵害通知制度中，主管機關之監管職責較為明顯，但仍是處於接收侵害事故相關資訊、決定是否提供協助之輔助性地位。

2、通知當事人與通報主管機關並行，主管機關居於主導地位

發生個資侵害事故時，通報主管機關之條件與通知當事人同等或更為嚴格，且主管機關可能對侵害事故通知當事人之時點與方式等享有監管權。

歐盟GDPR、日本個人資訊保護法及新加坡PDPA皆屬此類。歐盟 GDPR 原則要求一切個資侵害事故皆通報主管機關，且訂有嚴格時限，唯有侵害事故不致影響個資當事人權利與自由時方可免於通報。GDPR 關於通知當事人之要求，則注重保護當事人免受不必要的「通知疲勞」，以侵害事故「可能導致自然人權利和自由之高風險」為標準。依新加坡之個資侵害通知制度，通報主管機關與通知當事人標準相同，但要求組織在通報主管機關「同時或之後」，通知當事人，且主管機關得依職權或依申請，命令組織不得將侵害事故通知當事人。日本個人資訊保護法對於個資侵害事故通報主管機關與通知當事人標準相同，但通報主管機關有時限要求，通知當事人之時限則無明文規定

（二）個資侵害通知之可裁量性

依個資侵害通知與通報之標準是否包含事故發生機關之裁量判斷要素，可將我國及國外之個資侵害通知與通報制度大致分為以下幾類：

1、由侵害事故發生機關判斷個資侵害事故是否由其違反個資法之行為導致

本報告比較研究之國家中，這是我國獨有的個資侵害通知判斷事項。個資侵害事故發生後，事故發生機關應查明其是否違反個資法規定（不限違反何者規定），致使該個資侵害事故發生。若無法儘快查明，則依主管機關見解[247]，仍應從保障當事人利益出發，通知當事人。

[247] 見法務部 106 年 6 月 5 日法律字第 10603503230 號函。

2、由侵害事故發生機關判斷個資侵害事故是否可能導致當事人權益之風險或損害

歐盟、日本、美國維吉尼亞州和新加坡法律皆採此等判斷事項。前開各國資侵害通知與通報規範對於當事人權益侵害要求之標準固有差異（例如，歐盟 GDPR 對於通報主管機關時，所要求之風險標準極低，而日本、新加坡對於通報主管機關，仍限於高風險、嚴重損害），然觀察其相關規範可知，對當事人權益風險/損害之判斷要素，大致包括：侵害事故的類型，個人資料之性質、敏感性和數量，受影響之當事人數量，對當事人可能造成之影響等。

3、以客觀事實為判斷標準，不包含侵害事故發生機關裁量判斷要素

韓國和美國加州法律為此一類型。依據韓國個人資料保護法，若一般個人資料處理者發生個資外洩，或資訊與通訊服務提供者發生使用者資料滅失、竊盜或外洩，即生通知當事人和（或）通報主管機關之義務。依美國加州民法典，若符合法定條件之個資發生外洩，即生通知當事人之義務。

對於韓國和美國加州法律規定之應通知或通報個資侵害事故，侵害事故發生機關皆無裁量判斷空間。但從兩國（州）法律具體內容觀察，可發現其仍內含風險要素。日本與韓國將假名資料排除於個資侵害通知與通報制度外，可謂考量假名資料識別性較低，對當事人權益造成的風險較低。加州單純加密資訊（不含密鑰）排除於個資侵害通知與通報制度外，亦似基於對加密資料對當事人權益造成的風險較低之考量。

（三）個資侵害通知之例外

觀察前述包含當事人權益風險或損害判斷要素之個資侵害通知/通報制度，可知其包含共通之例外條件[248]，即侵害事故發生機關採取事前或事後之措施，防範風險實現/損害發生。此等措施通常具有技術性，如（複雜）加密等。

此外，日本與韓國的個資侵害通知與通報制度，不適用於已假名化處理之個人資料。此一例外亦包含風險相關考量，蓋妥適之假名化處理可降低個人資料之識別性，對當事人權益造成之風險也相應降低。

各國個資法規關於本議題之比較表格如下：

表 4、各國個資侵害事故通知相關規範比較表

國家	權利內容	法源依據	位階
臺灣	保有資料者違反個人資料保護法規範，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。	個人資料保護法第 12 條	法律
歐盟	1、 發生個資外洩事故時，控管者立即（至遲於知悉後 72 小時內）通報主管機關，但外洩難以影響個資當事人權利與自由時，不在此限。 2、 發生個資外洩事故且可能造成自然人權利的高風險時，控管者應盡快通知個資當事人。	GDPR§33-34	法律

[248] 此處所討論之例外，不包括通知當事人勞費過鉅或存在其他事實性困難之情形，蓋此等情形下，侵害事故發生機關仍應採取替代性通知措施，而非完全豁免通知義務。

國家		權利內容	法源依據	位階
美國	加州	1、 發生下列個資外洩事故後，個人資訊之持有人應立即通知個資當事人： (1) 外洩資訊未經加密； (2) 外洩資訊已經加密，但行為人可能取得密鑰。 2、 個資外洩事故影響超過 500 人時，個人資訊之持有人應通報州檢察長辦公室與個資當事人。	加州民法典 (Civil Code) §1798.82	法律
	維吉尼亞州	發生下列個資外洩事故後，個人資訊之持有人應立即通知州檢察長辦公室與個資當事人： (1) 外洩資訊未經加密； (2) 外洩資訊已經加密，但行為人可能取得密鑰。	維吉尼亞州法典 (Code of Virginia) §18.2-186.6	法律
日本		個資外洩事故存在個人權益侵害之高風險時，個資處理者應通報主管機關並通知個資當事人。	個人資訊保護法 §22-2	法律
韓國		1、 個人資料處理者知悉個資外洩事故時，應即時將外洩資料類別、救濟措施等通知資料當事人。 2、 個資外洩事故達到總統令所定規模時，須向主管機關通報。	個人資料保護法 §34	法律

國家	權利內容	法源依據	位階
新加坡	1、 由外部人員造成的個資外洩事故，如符合下列條件之一，組織應通知當事人： (1) 可能對個資當事人造成重大影響； (2) 可能具較大規模。 2、 下列情形下，組織得不通知當事人： (1) 外洩事故發生後，組織已採取措施，使事故不太可能對個資當事人造成重大影響； (2) 外洩事故發生前，組織已採取技術措施，使事故不太可能對個資當事人造成重大影響。 3、 個資法主管機關或執法機關得指示組織不向當事人通知。	PDPA §26A-E	法律

五、修法需求分析

承繼上述法規比較，我國個資法在個資侵害事故通知當事人方面，係以侵害事故發生機關之違法性作為判斷標準，未呈現對當事人權益風險之考量。

現行個資法規範個資侵害事故通知之第 12 條，係於民國 99 年修法時新增，其立法理由指出，「當事人之個人資料遭受違法侵害，往往無法得知，致不能提起救濟或請求損害賠償，爰規定公務機關

或非公務機關所蒐集之個人資料被竊取、洩漏、竄改或遭其他方式之侵害時，應立即查明事實，以適當方式，迅速通知當事人，讓其知曉」。

是故，我國個資法創設個資侵害事故通知制度之初衷，係使當事人知曉其個人資料已遭侵害之事實，並使其能夠僅適尋求救濟或採取其他因應措施。然現行個資法要求事故發生機關在判斷是否通知當事人時，考量侵害事故是否由其違反個資法之行為引起，而非對當事人權益是否將因此遭受損害、損害程度與急迫性如何，似與立法理由所述目標存有落差。

因此，我國或可思考調整現行通知當事人之判定標準，以歐盟、日本或新加坡等國相關規範為參考，引入當事人權益風險之考量要素。在依下文建議引入個資侵害事故通報制度的前提下，由於已由主管機關監督個資侵害事故之因應，宜以對當事人權益之「風險較高」作為通知當事人之門檻標準，以免對當事人造成「通知疲勞」。而風險之判斷，宜以客觀上對當事人隱私或其他權利之不利影響性質及其發生可能性為依據，由事故發生機關為初步判斷並據以決定是否通知當事人，並進而由收受事故通報之主管機關為進一步判斷，以核驗事故發生機關不予通知當事人（「非屬風險較高」）之適當性。如主管機關認有通知當事人之必要，得要求事故發生機關通知當事人。

而在通報主管機關方面，我國個資法並無個資侵害事故通報主管機關之明文規範，現行通報制度係由非公務機關之中央目的事業主管機關分別訂定，尚欠缺統一性通報標準。

如歐盟 GDPR 前言第 85 點所述，個資侵害事故如未及時適當處理，可能對當事人造成歧視、名譽損害、身分竊盜、財產損失等不利益。因此，要求事故發生機關將個資侵害事故通報主管機關，對於確保侵害事故迅速妥適因應、防範當事人權益受損有重要作用。

又依我國個資法第 48 條第 2 款，若非公務機關未依法將個資侵害事故通知當事人，主管機關得要求限期改正乃至處以罰鍰。然對

於諸多未建立個資侵害通報制度之行業，主管機關恐難以儘速掌握其對侵害事故之因應狀況並施以適當監管，當事人因侵害事故而權益受損之風險也相應提高。因此，我國似可考慮在個資法中增訂個資侵害事故通報規範，統一通報標準及程序，以利落實現行個資法保障個資當事人權益之立法目的。

為確保對事故發生機關因應狀況之有效監督、及時給予行政指導，我國個資法似可採納歐盟 GDPR 之標準，除不致影響當事人權益者外，原則應通報一切個資侵害事故。又資訊相關安全事故通報制度在我國法律中已有先例，我國於 107 年頒行資通安全管理法，建立資通安全事件通報制度。個資侵害事故與資通安全事件雖所涉對象不同，但兩者有密切關聯，個資侵害事故之發生，通常是資通安全事件之結果[249]。為整合我國資訊相關安全事故通報制度，提升個資侵害事故通報及因應之效率，個資侵害事故通報制度似宜與現行之資通安全事件通報制度調和一致。

詳言之，公務機關知悉個資侵害事故後，應通報上級或監督機關；非公務機關知悉個資侵害事故後，應通報中央目的事業主管機關。另一方面，前述分別通報上級機關或中央目的事業主管機關之制度，仍有個資侵害因應專業度及量能不足之隱憂。個資侵害事故之通報制度細部規範，宜由主管機關在擬訂個資法修正草案時，與個資法專責主管機關制度作通盤規劃。

而從國際發展趨勢觀察，各國對個資侵害通知與通報制度之重視程度正逐漸提高。本報告比較研究的國家中，日本與新加坡皆於 2020 年增修個資法律，引入強制性個資侵害通知/通報制度。其中新加坡於正式修法前，先行預告修法計畫並修訂相關指引，以協助個資蒐集處理利用機關適應法規變化，此修法策略或可作為我國參考。

[249] 例如，我國銓敘部於 2019 年發現發生第三級資通安全事件，約 58 萬筆公職人員個人資料外洩，詳見，監察院民國 109 年 1 月 16 日 109 教調 0004 號調查報告，頁 7。

六、本節結論

綜合本節比較研究，本報告發現，各國對個資侵害通知與通報制度之重視程度正逐漸提高，所研究之外國立法例中，皆兼具通知當事人及通報主管機關制度，惟其制度架構不同。

我國個資法在個資侵害事故通知當事人方面，係以侵害事故發生機關之違法性作為判斷標準，未呈現對當事人權益風險之考量。而在通報主管機關方面，我國個資法並無個資侵害事故通報主管機關之明文規範，現行通報制度係由非公務機關之中央目的事業主管機關分別訂定，尚欠缺統一性通報標準。

若要進一步落實現行個資法保障個資當事人權益之立法目的，於通知當事人面向，可思考調整現行判定標準，引入當事人權益風險之考量要素。於通報主管機關面向，可考慮於個資法中，規範個資侵害事故通報標準，構建個資侵害事故通報制度。又「行政院及所屬各機關落實個人資料保護聯繫作業要點」已明定非公務機關個資侵害事故通報之標準與程序，可以預期該要點將於正式修法前，對統一各目的事業之個資侵害事故制度有顯著促進之效。

第五節 當事人同意

一、議題釐清

本議題源於「臺灣開放政府國家行動方案」中的承諾事項 1-3「強化數位隱私與個資保護」[250]，由於「現行個資法雖規定「當事人（書面）同意」為蒐集、處理或利用合要件之一，惟目前採用之同意方式過於概括或所需同意之內容過於複雜，常發生爭議」，對此，本議題即須針對「個資法同意之意涵、要件明確性及配套措施（包括但不限於：當事人撤回其同意之時機與要件）」進行研議。

二、我國個人資料保護法

我國個資法雖未於第 2 條對「同意」之內涵加以定義，但於第 7 條第 1 項規定，當蒐集機關以「經當事人同意」作為「蒐集、處理（並於蒐集目的內利用）個人資料」的合法要件時，該同意係指「當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示」；又當蒐集機關以「經當事人同意」作為「目的外利用個人資料」的合法要件時，依同條第 2 項規定，該同意係指「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」，對此，個資法施行細則第 15 條並規定，所謂「單獨所為之意思表示」，如係與其他意思表示於同一書面為之者，蒐集者應於適當位置使當事人得以知悉其內容並確認同意。

另依個資法第 7 條第 3 項規定，在公務機關或非公務機關蒐集個人資料時，如已明確告知當事人個資法第 8 條第 1 項各款應告知事項，而當事人未表示拒絕，並已提供其個人資料者，即推定當事人已表示同意。

至於當事人同意之事實的舉證責任，依個資法第 7 條第 4 項規定，應由蒐集者負擔。

---

[250] 臺灣開放政府國家行動方案，2021 年 4 月，頁 12-15。

三、外國立法例

（一）歐盟 GDPR

當事人同意為歐盟 GDPR 第 6 條第 1 項第 a 款規定控管者得處理個人資料的合法要件之一（亦為第 9 條第 2 項第 a 款禁止處理特種個資的例外之一）。

依 GDPR 第 4 條第 11 款之定義[251]，當事人的「同意」是指當事人透過聲明或清楚肯定之行為，對處理其個人資料作出具備自主、特定、知情與明確而允許之意思表示。

為確保當事人以清楚肯定之行為表達同意，GDPR 前言第 32 點第 2 段與第 3 段指出[252]，清楚肯定之行為可包括瀏覽網站時勾選框格、使用資訊社會服務時選擇特定的技術設定，或其他清楚表示當事人接受處理其個人資料之請求的聲明或行動。至於沉默、預先勾選框格、不作為等方式，則不構成當事人之同意。

而在評估同意的自主性時，GDPR 第 7 條第 4 項規定[253]，應尤其考量契約之履行（包含服務之提供）是否以同意處理其個人資料作為條件，而該處理個資行為對契約之履行並無必要。GDPR 前言第 43 點並表示[254]，當控管者與當事人間存有明顯不對等關係（尤其控管者為公務機關）時，當事人的

[251] EU, GDPR, §4(11), "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

[252] EU, GDPR, Recital §32, "…This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent…

[253] EU, GDPR, §7(4), "When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

[254] EU, GDPR, Recital §43, "In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance."

同意不太可能具有自主性；且如當事人無法對不同處理個人資料之行為分別表達同意，或儘管履行契約非以當事人同意處理其個人資料為必要，但控管者仍以同意（處理個人資料）為契約履行（包含提供服務）的條件時，該同意應推定為不具自主性。

另 GDPR 第 7 條第 2 項規定[255]，如當事人之同意係併同其他事項所為之書面聲明時，應以明確與其他事項區分的形式向當事人徵求同意，並使用易懂且便於取得之格式，以及清楚簡白之語言。該聲明中任何違反歐盟 GDPR 之部分均屬無效。

同條第 3 項規定[256]，當事人應有權隨時撤回同意，但其撤回不影響撤回前基於該同意處理個人資料的合法性。當事人應於同意前即受告知有前述撤回之權。且同意之撤回應與表達同意一樣容易。

最後，GDPR 第 7 條第 1 項規定[257]，當控管者以當事人同意作為處理個人資料的依據時，應由控管者就當事人同意該處理行為的事實負舉證之責。

除 GDPR 的明文外，歐盟個資保護委員會（EDPB）發布之《關於 GDPR 中的同意之指引（以下稱 GDPR 同意指引）》補充解釋說明[258]，若當事人未能獲得真正的選擇，或受到強迫而作出同意，或如不同意將使其遭受負面後果時，該同意即為無效。又如將同意綑綁於契約條款中，成為無法磋商的

[255] EU, GDPR, §7(2), "If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding."

[256] EU, GDPR, §7(3), "The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent."

[257] EU, GDPR, §7(1), "Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data."

[258] 見 EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, 4 May 2020, version 1.1.

一部分時，即推定為不具自主性。因此，若當事人無法拒絕或撤回同意而免受任何不利益時，其同意即不被認為具備自主性。

此外，對當事人造成不適當之壓力或影響，進而使當事人無法行使自由意願時，亦將導致同意無效。例如：

1、權力不對等

如在僱傭關係中，鑒於雇主與受雇人之間的從屬性，當事人不太可能可拒絕同意雇主處理其個人資料，而毋庸面臨因拒絕所致不利影響的恐懼或實際風險。舉例來說，當雇主要求同意在工作場所啟用例如攝影監視等監控機制，或要求填寫評估表格時，受雇人不太可能可自由回覆同意與否而不感到壓力。

2、將同意作為條件

將同意與接受條款或條件「綑綁」，或當處理個人資料並非某契約或服務所必要，卻將提供契約或服務與徵求處理個資之同意「綑綁」一起的情形，當事人的同意都將被視為不具備自主性。

3、無法區分不同目的給予同意

某項服務可能包含不只一種目的之處理個資行為。在此情形，當事人應可自由選擇接受何種目的，而無須一次同意所有目的。若徵求同意的過程並不允許當事人就各別處理個資行為分別給予同意（例如只同意某些行為，不包含其他），儘管在個案中尚屬適當，該同意仍將推定為不具備自主性。

4、不同意將造成額外不利益

控管者必須證明當事人拒絕或撤回同意不會導致任何額外不利益，否則該同意將被認為不具備自主性。

《GDPR 同意指引》另認為，當事人的同意必須針對「一個或數個特定的」目的而作成，且當事人對各別目的均有選擇權，此原則是為確保當事人之控制權及透明性的程度，且密切與「知情性」的規範相連結，且亦應滿足前述「自主性」中的「可區分不同目的給予同意」的要件。此「特定性」的要求結合「目的限制」的法律原則，可避免控管者或第三人在當事人預期範圍之外利用其個人資料，始當事人失去控制權[259]。

又為讓當事人得在知情前提下作出決定，瞭解自己同意的內容，並行使例如撤回同意等權利，事先在獲得其同意前提供必要資訊極為重要。《GDPR 同意指引》即說明，若控管者未提供可取得的資訊，當事人的控制權即形同虛設，而其作出的同意將認定為不具效力。

同時，徵求同意（揭露必要資訊）所使用的文字應清楚、簡白，即通常一般之人均可輕易理解；且不可採用冗長而難以理解的隱私權政策或充滿法律用語的聲明。又同意必須清晰且可與其他事項有所區隔，並以可理解且可輕易取得的方式提供。此規範實質上表示，不可將與同意與否的知情決定有關之資訊隱藏於一般的契約條款。

當同意的請求是（書面）契約的一部分時，該請求應清楚與其他事項區別。如書面契約包含與同意使用個人資料無關的事項時，對於同意事項應清楚突顯，或呈現於另一份文件。同樣的，如經由電子方式徵求同意，該同意之請求應分列並有所區別，不可僅作為契約條款的一個段落。考慮到小

[259] GDPR 對此特定性要求，在科學研究目的下有所放寬。GDPR 前言第 33 點指出「通常不太可能在資料蒐集時，便完整識別為科學研究而運用個人資料之目的。因此，如符合科學研究公認的倫理標準時，應允許當事人僅就特定範圍的科學研究給予同意。當事人應有機會僅對特定研究範圍或預期目的允許範圍內的部分研究計畫給予同意」；《GDPR 同意指引》並補充認為，當無法完整指明研究目的時，控管者應尋求其他方式以確保最大程度滿足同意的規範意旨，例如允許當事人以較概略方式同意研究目的，以及同意一開始即知的研究計畫之特定階段。隨著研究的進展，便可在下一階段開始前獲得對該計畫後續步驟的同意。不過，該同意仍應符合科學研究適用的倫理標準。

螢幕或僅有有限空間揭露資訊的情形，如適當時，可考慮採用階層方式呈現資訊，以避免對使用者體驗或產品設計造成過度干擾。

此外，《GDPR 同意指引》強調，GDPR 要求同意須經由積極行動或聲明而提出。因此，使用預先勾選同意加入的框格是無效的。當事人的單純沉默、不作為或繼續使用服務之行為，均不可視為對其選擇的積極表示。控管者應以對當事人足夠清晰的方式設計同意機制，避免任何模糊空間，並確保給予同意之行為可與其他行為有所區別，僅是繼續使用網站並不可推論為當事人對處理個人資料的行為表達同意的意思表示。

最後，《GDPR 同意指引》主張，雖然 GDPR 僅規定控管者應確保當事人得以作成同意相同簡易的方式，在任何特定時間撤回其同意，並未要求作成和撤回同意必須透過同樣的動作完成。但在實作中，當同意是以一鍵點擊滑鼠、滑動或按鍵等電子方式獲得時，當事人必須可以相同簡易的方式撤回該同意。又如同意是藉由使用該服務特定的使用者界面（例如透過網站、應用程式、登入帳號、物聯網裝置的界面或電子郵件）而獲得時，當事人須可以相同的電子界面撤回同意，不應讓當事人為撤回同意而須切換至其他界面。另當事人撤回同意時，應有權免受不利益，即控管者應尤其盡可能使撤回同意無需付費或不致降低現有服務的水平。

（二）美國加州 CCPA

加州 CCPA 並未就業者蒐集、利用消費者個人資訊定有整體性的前提要件（例如我國個資法第 15 條與第 19 條、歐盟 GDPR 第 6 條等），但消費者之同意仍在 CCPA 中發揮消費者自主控制其個人資訊之作用。

依 CCPA 第 1798.120 條第 d 項規定[260]，消費者同意乃加州 CCPA 允許業者販售或分享未成年消費者個人資訊，或在消費者選擇退出（opt out）即拒絕業者販售或分享其個人資料後，再次販售或分享其個人資訊之依據。

又依第 1798.121 條第 b 項規定[261]，消費者同意亦為業者在消費者限制業者僅得為特定目的利用或揭露其敏感個人資訊後，再次為其他目的而利用或揭露其敏感個人資訊之依據。

此外，如業者以財務激勵作為蒐集、販售、分享或保存消費者個人資訊的對價時，依第 1798.125 條第 b 項第 3 款規定[262]，消費者的（事前）知情同意即為該行為的合法要件，且消費者須有權隨時撤回同意。

而依 CCPA 第 1798.140 條第 h 項之定義[263]，「同意」是指消費者（或其法定代理人、有權代理之人，或監護人）透過聲明或清楚肯定之行為，針對為嚴謹定義之特定目的而處

[260] California, CCPA (as amended by CPRA), §1798.120(d), "A business that has received direction from a consumer not to sell or share the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell or share the minor consumer's personal information, shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from selling or sharing the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides consent, for the sale or sharing of the consumer's personal information."

[261] California, CCPA (as amended by CPRA), §1798.121(b), "A business that has received direction from a consumer not to use or disclose the consumer's sensitive personal information, except as authorized by subdivision (a), shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from using or disclosing the consumer's sensitive personal information for any other purpose after its receipt of the consumer's direction unless the consumer subsequently provides consent for the use or disclosure of the consumer's sensitive personal information for additional purposes."

[262] California, CCPA (as amended by CPRA), §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 1798.130 that clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time. If a consumer refuses to provide opt-in consent, then the business shall wait for at least 12 months before next requesting that the consumer provide opt-in consent, or as prescribed by regulations adopted pursuant to Section 1798.185."

[263] California, CCPA (as amended by CPRA), §1798.140, " (h) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent."

理與其有關的個人資訊之行為，作出具備自主性、特定性、知情性與明確性而允許之意思表示。接受一般性或廣泛性的使用條款或類似文件，其中包含處理個人資料的說明及其他不相關的資訊者，不構成同意。游標懸停（hovering over）、沉默、暫停、關閉內容亦不構成同意。同樣的，以不正方式（dark patterns，指經設計或操縱而會對使用者自主、決策或選擇造成破壞或減損等重大影響的使用者界面[264]）取得之允許也不構成同意。

（三）美國維吉尼亞州 CDPA

消費者同意乃維吉尼亞州 CDPA 中，控管者於目的外處理個人資料或處理敏感資料的前提要件。CDPA 第 59.1-574 條第 A 項第 2 款規定[265]，除另有規定外，控管者非得消費者同意，不得為「與其向消費者揭露之蒐集目的既不合理必要（reasonably necessary）也不相容（compatible）」之目的而處理個人資料；同項第 5 款前段則規定[266]，未得消費者同意，控管者不得處理該消費者的敏感資料。

依 CDPA 第 59.1-571 條中的定義[267]，同意是指消費者對處理與其有關的個人資料所表達具有自主性、特定性、知情性與明確性而允許之意的清楚肯定之行為，包含電子文件在內的書面聲明或其他明確肯定的行動。

[264] California, CCPA (as amended by CPRA), §1798.140, "(l) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation."

[265] Virginia, CDPA, §59.1-574(A)(2), "A controller shall:…2. Except as otherwise provided in this chapter, not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent".

[266] Virginia, CDPA, §59.1-574(A)(5), "A controller shall:…5. Not process sensitive data concerning a consumer without obtaining the consumer's consent…".

[267] Virginia, CDPA, §59.1-571, "'Consent' means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action."

（四）日本個人資訊保護法

當事人同意乃日本個人資訊保護法於第 16 條第 1 項規定，允許個人資訊處理事業於目的外處理個人資訊之要件[268]。該法未於條文中對當事人「同意」具體定義，但日本個資保護委員會於「個人資訊保護法指引（通則編）」第 2 章第 2-16 節對於「同意」提供解釋。

依指引說明[269]，同意是指當事人本人同意個人資訊處理事業依其規定之處理方式，處理其個人資訊的意思表示（以可確認當事人為本人為前提）；而取得當事人之同意則指個人資訊處理事業明確瞭解當事人所為允許之意思表示。在考量業務性質與個人資料處理狀況的前提下，當事人須以必要之合理及適當方式作出同意之決定。

該指引亦舉出數個當事人有效同意的示例，包含：口頭表示同意、書面同意(包含電磁紀錄)、電子郵件表示同意、勾選確認欄表示同意、點擊頁面按鈕同意與輸入語音、碰觸觸控面板、按鈕、開關等。

經數位社會整備法修正後，前開規範雖有條號及文字調整，但其內容並無實質變化。

值得注意者，日本公平交易委員會於 2019 年發布《數位平台營運者對提供個人資訊之消費者的濫用相對優勢地位行為指引（デジタル・プラットフォーム事業者と個人情報等を提供する消費者との取引における優越的地位の濫用に関する独占禁止法上の考え方）》[270]，將數位平台營運者（指經營社群網站服務、線上購物商城、app 市集、搜尋服務、提

[268] 日本，個人情報保護法，§16(1)，「個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない」。

[269] 見日本，個人情報保護委員会，平成 28 年 11 月（令和 3 年 8 月一部改正），個人情報の保護に関する法律についてのガイドライン（通則編），第 25-26 頁。

[270] 見 https://www.jftc.go.jp/houdou/pressrelease/2019/dec/191217_dpfgl_11.pdf，最後到訪為 110 年 11 月 2 日。

供數位內容如圖片、影像、音樂、電子書等業者）利用「相對（市場）優勢地位」及「資訊不對稱」而蒐集或利用消費者個人資訊之行為，列為不公平競爭的範圍。

該指引即指出，若消費者因為沒有替代選項而只能使用某企業之服務，且被該企業要求必須「同意提供目的必要範圍外之其他個人資訊」，或「同意該企業於目的必要範圍外之其他利用個人資訊行為（例如精準行銷或提供個人資訊予第三人」，否則便無法獲得服務時，消費者的同意可能遭認定非出於自願，將使該企業構成不正蒐集或利用個人資訊之行為。

（五）韓國個人資料保護法

當事人同意為韓國個人資料保護法第 15 條第 1 項第 1 款規定蒐集（並於蒐集目的內利用）個人資料之合法要件[271]，同條第 2 項規定[272]，個人資料處理者以當事人同意為依據時，應向當事人告知下列資訊，如日後有任何變更時，應再向當事人告知並取得同意：(1)個人資料的蒐集與利用目的；(2)蒐集個人資料之項目（義同類別）；(3)保有及利用個人資料的期間；(4)有權利拒絕同意之事實，以及拒絕同意如將受不利益時，該不利益之內容。

[271] 한국，개인정보보호법，§15(1)①，「개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다. 1. 정보주체의 동의를 받은 경우」。

[272] 한국，개인정보보호법，§15(2)，「개인정보처리자는 제 1 항제 1 호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다. 1. 개인정보의 수집·이용 목적 2. 수집하려는 개인정보의 항목 3. 개인정보의 보유 및 이용 기간 4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용」。

第 16 條第 2 項規定[273]，個人資料處理者在取得當事人同意時，應具體向當事人告知其可拒絕同意個人資料處理者蒐集最小必要範圍以外的個人資料，始得蒐集個人資料；且依同條第 3 項規定[274]，個人資料處理者不得以當事人拒絕同意蒐集最小必要範圍以外之個人資料為由，拒向當事人提供商品或服務。

另依韓國個人資料保護法第 17 條第 1 項第 1 款規定[275]，當事人同意可作為個人資料處理者將個人資料提供予第三方（包含共同利用）的合法要件，同條第 2 項規定[276]，個人資料處理者在取得同意時，應向當事人告知下列資訊，如日後有任何變更時，應再向當事人告知並取得同意：(1)個人資料之接收者；(2)個人資料接收者利用該個人資料之目的；(3)提供個人資料的項目（義同類別）；(4)個人資料接收者保有及利用該個人資料的期間；(5)有權拒絕同意之事實，以及拒絕同意如將受不利益時，該不利益之內容。

---

273 한국，개인정보보호법，§16(2)，「개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다.」。

274 한국，개인정보보호법，§16(3)，「인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.」。

275 한국，개인정보보호법，§17(1)①，「개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제 3 자에게 제공(공유를 포함한다. 이하 같다)할 수 있다. 1. 정보주체의 동의를 받은 경우」。

276 한국，개인정보보호법，§17(2)，「개인정보처리자는 제 1 항제 1 호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다. 1. 개인정보를 제공받는 자 2. 개인정보를 제공받는 자의 개인정보 이용 목적 3. 제공하는 개인정보의 항목 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용」。

又依韓國個人資料保護法第 18 條第 2 項第 1 款規定[277]，個人資料處理者如自當事人取得別途同意[278]，可於蒐集目的外利用個人資料或提供予第三方。此時，同條第 3 項規定[279]，個人資料處理者應向當事人告知下列資訊，如日後有任何變更時，應再向當事人告知並取得同意：(1)個人資料接收者；(2)個人資料之利用目的（於提供第三方之情形，接收者於接收時之利用目的）；(3)被利用或被提供的個人資料項目（義同類別）；(4)保有及利用個人資料的期間（於提供第三方之情形，接收者於接收時之保有及利用期間）；(5)有權拒絕同意之事實，以及拒絕同意如將受不利益時，該不利益之內容。

而韓國個人資料保護法於第 22 條規定同意取得之辦法，依第 1 項規定[280]，個人資料處理者在取得當事人同意時，應以清楚可辨的方式，將個別同意事項分開呈現，並分別取得

---

277 한국，개인정보보호법，§18(2)(1)，「제 1 항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제 3 자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제 3 자에게 제공할 수 있다. 다만, 이용자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제 2 조제 1 항제 4 호에 해당하는 자를 말한다. 이하 같다)의 개인정보를 처리하는 정보통신서비스 제공자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제 2 조제 1 항제 3 호에 해당하는 자를 말한다. 이하 같다)의 경우 제 1 호・제 2 호의 경우로 한정하고, 제 5 호부터 제 9 호까지의 경우는 공공기관의 경우로 한정한다. 1. 정보주체로부터 별도의 동의를 받은 경우」。

278 별도的漢字為「別途」，即另外用途、其他用途之意，此應指目的外利用個人資料之同意。

279 한국，개인정보보호법，§18(3)，「개인정보처리자는 제 2 항제 1 호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다. 1. 개인정보를 제공받는 자 2. 개인정보의 이용 목적(제공 시에는 제공받는 자의 이용 목적을 말한다) 3. 이용 또는 제공하는 개인정보의 항목 4. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다) 5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용」。

280 한국，개인정보보호법，§22(1)，「개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제 6 항에 따른 법정대리인을 포함한다. 이하 이 조에서 같다)의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다.」。

當事人同意。第 2 項規定[281]，個人資料處理者以書面（含電子文件）取得同意時，就大統領令所定之重要內容（目的、項目等），應依個資保護委員會告示之辦法，明確標示使其簡單明瞭。

另依同條第 3 項規定[282]，個人資料處理者基於當事人同意而蒐集、利用個人資料或提供予第三方時，應區別基於履行與當事人間契約等目的，而無當事人同意仍可處理之個人資料，以及須經當事人同意始得處理之個人資料（此時，未經同意即可處理之個人資料應由個人資料處理者負舉證責任）。

又同條第 4 項規定[283]，個人資料處理者為向當事人宣傳商品或服務，或引誘販售，而欲取得處理個人資料之同意時，應告知使當事人明確知悉該情事並取得同意。

同條第 5 項則規定[284]，個人資料處理者不得以當事人拒絕前述第3項選擇同意事項，或拒絕同意第4項（行銷）及第18條第2項第1款（目的外利用）為由，拒向當事人提供商品或服務。

---

281 한국，개인정보보호법，§22(2)，「개인정보처리자는 제 1 항의 동의를 서면(「전자문서 및 전자거래 기본법」 제 2 조제 1 호에 따른 전자문서를 포함한다)으로 받을 때에는 개인정보의 수집・이용 목적, 수집・이용하려는 개인정보의 항목 등 대통령령으로 정하는 중요한 내용을 보호위원회가 고시로 정하는 방법에 따라 명확히 표시하여 알아보기 쉽게 하여야 한다.」。

282 한국，개인정보보호법，§22(3)，「개인정보처리자는제 15 조제 1 항제 1 호, 제 17 조제 1 항제 1 호, 제 23 조제 1 항제 1 호및제 24 조제 1 항제 1 호에따라개인정보의처리에대하여정보주체의동의를받을때에는정보주체와의계약체결등을위하여정보주체의동의없이처리할수있는개인정보와정보주체의동의가필요한개인정보를구분하여야한다. 이경우동의없이처리할수있는개인정보라는입증책임은개인정보처리자가부담한다.」。

283 한국，개인정보보호법，§22(4)，「개인정보처리자는 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 때에는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.」。

284 한국，개인정보보호법，§22(5)，「개인정보처리자는 정보주체가 제 3 항에 따라 선택적으로 동의할 수 있는 사항을 동의하지 아니하거나 제 4 항 및 제 18 조제 2 항제 1 호에 따른 동의를 하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.」。

至於當個人資料處理者欲處理 14 歲以下兒童之個人資料而需取得同意時，第 22 條第 6 項規定[285]，個人資料處理者應取得其法定代理人之同意。此時，得未經法定代理人同意，直接向該兒童蒐集「為取得法定代理人同意所需」最小必要範圍之資料。

（六）新加坡個人資料保護法

當事人之「同意」或「視為同意」乃新加坡個人資料保護法第 13 條第(a)款規定組織得蒐集、利用或揭露個人資料的合法要件之一[286]。

依新加坡個人資料保護法第 14 條第 1 項規定[287]，當事人同意以「該當事人經告知本法第 20 條所列資訊（特定目的）」且「該當事人依本法規定對此目的給予同意」為要件。

同條第 2 項並規定[288]，組織不得逾越向當事人提供產品或服務的合理範圍，將當事人同意蒐集、利用或揭露個人資料作為提供產品或服務的條件；組織亦不得以不實或誤導之資訊，或使用欺瞞或誤導的方法，取得或試圖取得當事人對

[285] 한국，개인정보보호법，§22(6)，「개인정보처리자는 만 14 세 미만 아동의 개인정보를 처리하기 위하여 이 법에 따른 동의를 받아야 할 때에는 그 법정대리인의 동의를 받아야 한다. 이 경우 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다.」。

[286] Singapore, PDPA, §13(a), "An organisation shall not, on or after the appointed day, collect, use or disclose personal data about an individual unless —(a)the individual gives, or is deemed to have given, his consent under this Act to the collection, use or disclosure, as the case may be…"

[287] Singapore, PDPA, §14(1),"An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless —(a)the individual has been provided with the information required under section 20; and(b)the individual provided his consent for that purpose in accordance with this Act."

[288] Singapore, PDPA, §14(2), "An organisation shall not —(a)as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about the individual beyond what is reasonable to provide the product or service to that individual; or(b)obtain or attempt to obtain consent for collecting, using or disclosing personal data by providing false or misleading information with respect to the collection, use or disclosure of the personal data, or using deceptive or misleading practices."

蒐集、利用或揭露個人資料之行為的同意。若有違反，依第3項規定[289]，該同意即屬無效。

新加坡個人資料保護法另有「視為同意（deemed consent）」之規定。依第15條第1項[290]，當事人雖未依第14條規定給予同意，但其自願為特定目的提供個人資料予該組織，且可合理認為該當事人確會自願提供該資料時，即視為當事人同意該組織基於特定目的而蒐集、利用或揭露其個人資料。而在當事人同意或視為同意組織基於特定目的，揭露其個人資料予其他組織時，依同條第 2 項規定[291]，即視為該當事人同意該其他組織基於特定之目的蒐集、利用或揭露其個人資料。

第 15 條第 3 項復規定締約階段之「視為同意」[292]，當事人 P 與某組織 A 締結契約而提供個人資料者，視為同意在與該組織 A 締結契約的合理必要範圍內之下列行為：(a)組織 A 得向其他組織 B 揭露當事人的個人資料；(b)組織 B 得蒐集與利用其個人資料；(c)組織 B 得再向其他組織揭露其個人資料。此時依同條第 4 項規定[293]，自組織 B 蒐集個人資料的其他組織，即認定為係由組織 A 依第 3 項第(a)款向其揭露個人資料，並可適用第 3 項第(b)款與第(c)款之規定。

---

[289] Singapore, PDPA, §14(3), "Any consent given in any of the circumstances in subsection (2) is not validly given for the purposes of this Act."

[290] Singapore, PDPA, §15(1),"An individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation for a purpose if —(a)the individual, without actually giving consent referred to in section 14, voluntarily provides the personal data to the organisation for that purpose; and(b)it is reasonable that the individual would voluntarily provide the data."

[291] Singapore, PDPA, §15(2),"If an individual gives, or is deemed to have given, consent to the disclosure of personal data about the individual by one organisation to another organisation for a particular purpose, the individual is deemed to consent to the collection, use or disclosure of the personal data for that particular purpose by that other organisation."

[292] Singapore, PDPA, §15(3),"Without limiting subsection (2) and subject to subsection (9), an individual (P) who provides personal data to an organisation (A) with a view to P entering into a contract with A is deemed to consent to the following where reasonably necessary for the conclusion of the contract between P and A:(a) the disclosure of that personal data by A to another organisation (B);(b)the collection and use of that personal data by B;(c)the disclosure of that personal data by B to another organisation."

[293] Singapore, PDPA, §15(4),"Where an organisation collects personal data disclosed to it by B under subsection (3)(c), subsection (3)(b) and (c) applies to the organisation as if the personal data were disclosed by A to the organisation under subsection (3)(a)."

另第 15 條第 6 項規定契約履行階段之「視為同意」[294]，當事人 P 與某組織 A 締結契約，並依該契約或與該契約有關而提供個人資料者，視為同意下列行為：(a)組織 A 得於合理必要範圍內，揭露其個人資料予其他組織 B，前提係(1)為履行 P 與組織 A 之契約，或(2)依 P 之要求或理性之人可認為係為 P 之利益，為組織 A 與組織 B 締結或履行契約；(b)當蒐集與利用其個人資料係為前(a)款目的而合理必要時，組織 B 得蒐集與利用其個人資料；(c)當揭露其個人資料係為第(a)款目的而合理必要時，組織 B 得向其他組織揭露其個人資料。此時依同條第 7 項規定[295]，自組織 B 蒐集個人資料的其他組織，即認定係由組織 A 依第 6 項第(a)款向其揭露個人資料，並可適用第 6 項第(b)款與第(c)款之規定。

此外，依新加坡個人資料保護法第 15A 條第 2 項規定[296]，除另有規定外，當滿足下列條件時，即視為當事人同意組織蒐集、利用或揭露其個人資料：(a)組織符合第 4 項規定，且(b)當事人未在第 4 項第(b)款第 3 目所定期限屆滿前，向組織通知其不同意組織所欲蒐集、利用或揭露該個人資料之行為。

而依第 15A 條第 4 項規定[297]，為第 2 項第 a 款目的，組織須在蒐集、利用或揭露該當事人的任何個人資料前：(a)對擬

[294] Singapore, PDPA, §15(6),"Without limiting subsection (2) and subject to subsection (9), an individual (P) who enters into a contract with an organisation (A) and provides personal data to A pursuant or in relation to that contract is deemed to consent to the following:(a)the disclosure of that personal data by A to another organisation (B), where the disclosure is reasonably necessary —(i)for the performance of the contract between P and A; or(ii)for the conclusion or performance of a contract between A and B which is entered into at P's request, or which a reasonable person would consider to be in P's interest;(b)the collection and use of that personal data by B, where the collection and use are reasonably necessary for any purpose mentioned in paragraph (a);(c)the disclosure of that personal data by B to another organisation, where the disclosure is reasonably necessary for any purpose mentioned in paragraph (a)."

[295] Singapore, PDPA, §15(7),"Where an organisation collects personal data disclosed to it by B under subsection (6)(c), subsection (6)(b) and (c) applies to the organisation as if the personal data were disclosed by A to the organisation under subsection (6)(a)."

[296] Singapore, PDPA, §15A(2),"Subject to subsection (3), an individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation if —(a)the organisation satisfies the requirements in subsection (4); and(b)the individual does not notify the organisation, before the expiry of the period mentioned in subsection (4)(b)(iii), that the individual does not consent to the proposed collection, use or disclosure of the personal data by the organisation."

[297] Singapore, PDPA, §15A(4),"For the purposes of subsection (2)(a), the organisation must, before collecting, using or disclosing any personal data about the individual —(a)conduct an assessment to

進行的個人資料蒐集、利用或揭露行為執行評估，以確認該行為不致對當事人產生不利影響；(b)採取合理步驟以向當事人提示下列資訊：(1)組織欲蒐集、利用或揭露該個人資料之意圖；(2)蒐集、利用或揭露該個人資料之目的；(3)當事人得向組織通知其不同意組織所欲蒐集、利用或揭露該個人資料之行為的合理期間與合理方式；(c)滿足其他任何明文規範。

又依第 16 條第 1 項規定[298]，當事人得隨時給予組織合理期限，就該組織基於任何目的蒐集、利用或揭露其個人資料之行為，撤回任何曾給予的同意或依本法規定的視為同意。

同條第 2 項規定[299]，該組織在接獲通知時，應向該當事人說明撤回同意可能產生的後果。且依第 3 項規定[300]，組織不得禁止當事人就蒐集、利用或揭露其個人資料之行為撤回同意，但其撤回不影響任何致生的法律後果。

四、法規比較

由上述法規可知，雖然並非各國個人資料保護法律均對「同意」之內涵有所定義，但包含我國個資法在內，均於法律條文或主管機關的指引中對於「同意」定有條件，顯見各國對於有效的當事人同意皆注重其特定品質。以歐盟 GDPR、美國加州 CCPA 與維吉尼亞州 CDPA 均於法律中明文規範的定義來看，有效的同意應以具備的「自主性」、「特定性」、「知情性」與「明確性」為條件：

---

determine that the proposed collection, use or disclosure of the personal data is not likely to have an adverse effect on the individual;(b)take reasonable steps to bring the following information to the attention of the individual:(i) the organisation's intention to collect, use or disclose the personal data;(ii)the purpose for which the personal data will be collected, used or disclosed;(iii) a reasonable period within which, and a reasonable manner by which, the individual may notify the organisation that the individual does not consent to the organisation's proposed collection, use or disclosure of the personal data; and(c) satisfy any other prescribed requirements."

[298] Singapore, PDPA, §16(1),"On giving reasonable notice to the organisation, an individual may at any time withdraw any consent given, or deemed to have been given under this Act, in respect of the collection, use or disclosure by that organisation of personal data about the individual for any purpose."

[299] Singapore, PDPA, §16(2),"On receipt of the notice referred to in subsection (1), the organisation concerned shall inform the individual of the likely consequences of withdrawing his consent."

[300] Singapore, PDPA, §16(3),"An organisation shall not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual, but this section shall not affect any legal consequences arising from such withdrawal."

（一）自主性

同意必須出於當事人完全的自主、自願，前述歐盟《GDPR 同意指引》認為，若當事人未能獲得真正的選擇，或受到強迫而作出同意，或如不同意將使其遭受負面後果時，該同意即為無效。又如將同意綑綁於契約條款中，成為無法磋商的一部分時，即推定為不具自主性。

依歐盟 GDPR 第 7 條第 4 項規定與前言第 43 點之說明可知，在評估同意的自主性時，應尤其考量契約之履行（包含服務之提供）是否以同意處理其個人資料作為條件，倘履行契約非以當事人同意處理其個人資料為必要，但控管者仍以同意（處理個人資料）為契約履行（包含提供服務）的條件時，該同意應推定為不具自主性；又當控管者與當事人間存有明顯不對等關係時，當事人的同意亦不太可能具有自主性；且如當事人無法對不同處理個人資料之行為分別表達同意時，該同意也應推定為不具自主性。

韓國個人資料保護法第 15 條第 3 項禁止個人資料處理者以當事人拒絕同意蒐集最小必要範圍以外之個人資料為由，拒向當事人提供商品或服務。第 22 條第 5 項亦規定，個人資料處理者不得以當事人拒絕前述第 3 項選擇同意事項，或拒絕同意第 4 項（行銷）及第 18 條第 2 項第 1 款（目的外利用）為由，拒向當事人提供商品或服務；新加坡個人資料保護法亦於第 14 條第 2 項第 a 款規定，組織不得逾越向當事人提供產品或服務的合理範圍，將當事人同意蒐集、利用或揭露個人資料作為提供產品或服務的條件。

上述規範均是強調當事人同意的自由性，任何帶有心理負擔之同意，皆不應認為構成有效之同意。

（二）特定性

同意須針對單項特定目的所為，若當事人無法針對不同目的分別表示同意與否之意，即有可能減損同意的自主性。

依歐盟 GDPR 第 7 條第 2 項規定，如當事人之同意係併同其他事項所為之書面聲明時，應以明確與其他事項區分的形式向當事人徵求同意，並使用易懂且便於取得之格式，以及清楚簡白之語言。

美國加州 CCPA 第 1798.140 條第 h 項對同意之定義亦認為，消費者如僅是接受一般性或廣泛性的使用條款或類似文件，其中包含處理個人資料的說明及其他不相關的資訊者，不構成有效的同意。

韓國個人資料保護法第 22 條第 1 項也要求個人資料處理者在取得同意時，應以清楚可辨的方式，將個別同意事項分開呈現，並分別取得當事人同意；新加坡個人資料保護法第 14 條第 1 項第 b 款亦規定，當事人同意以該當事人對特定目的給予同意為要件。

我國亦有類似見解，個資法主管機關曾認為[301]，如電信公司欲於單一業務申請書中，採當事人書面同意方式行銷業務[302]，建議於申請書中以較為顯著字體標示，與申請書中其他條款文句相區隔，並於獨立顯著位置予當事人表示同意與否之意思。金融監督管理委員會亦曾表示[303]，銀行業將告知書與同意書列於同一書面，未明顯區隔，易造成客戶混淆，而為概括同意。為避免客戶混淆，銀行業執行個資法第 8 條之告知說明，與同法第 19 條之取得當事人書面同意，宜於不同書面為之。

[301] 見法務部 101 年 12 月 10 日法律字第 10103107080 號函。
[302] 本函釋作成於 101 年 12 月 10 日，當時個資法第 20 條第 1 項但書第 6 款仍以「書面」為當事人同意蒐集者目的外利用個人資料之形式要件。
[303] 見金融監督管理委員會 101 年 10 月 24 日金管銀合字第 10130002690 號函。

（三）知情性

同意的「知情性」與法律對蒐集者要求的「透明性」互為搭配。比較法各國均課予蒐集者向當事人告知特定資訊之義務此亦為當事人同意應具備之條件。

歐盟 GDPR、美國加州 CCPA 與維吉尼亞州 CDPA 均將同意的「知情性」明文規定於法條之中；韓國個人資料保護法第 15 條第 2 項、第 17 條第 2 項、第 18 條第 3 項等，均要求個人資料處理者在取得當事人同意（蒐集、提供予第三方、目的外利用）時，須向當事人告知特定資訊，且第 22 條第 2 項規定，個人資料處理者以書面（含電子文件）取得同意時，就大統領令所定之重要內容（目的、項目等），應依個資保護委員會告示之辦法，明確標示使其簡單明瞭；新加坡個人資料保護法第 14 條第 1 項第 a 款亦規定，當事人同意以該當事人經告知特定資訊為要件。

我國個資法第 7 條第 1 項與第 2 項同樣要求蒐集者在以「當事人同意」作為蒐集或目的外利用個人資料的合法要件時，須向當事人明確告知法定資訊。

個資法主管機關更曾表示[304]，個資法第 7 條第 1 項規定（…第 19 條第 1 項第 5 款所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示）與第 8 條第 1 項規定（公務機關或非公務機關依第 15 條或第 19 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：…），其立法理由係以同意對於當事人權益有重大影響，自應經明確告知應告知事項，使當事人充分瞭解後審慎為之。教材業者欲基於當事人同意，蒐集未成年學童之個人資料，除應注意業者以贈品誘使學童提供個人資料，是否已違反個資法第 5 條之誠實信用原則外，業者另應踐行個資法第 8 條第 1 項相關

[304] 見國家發展委員會 108 年 3 月 12 日發法字第 1082000384 號函。

法定應告知事項，徵諸上開立法理由，應使當事人得以充分瞭解後審慎為之，是業者之告知方式應符合學童之年齡、生活經驗及理解能力，以容易理解、清楚簡單之語言或文字為之，並使該學童得以充分瞭解其個人資料之後續利用。倘教材業者未完整踐行告知，或其告知對象無法充分瞭解其個人資料之後續利用，則未能符合個資法第 7 條第 1 項之規定。

此函釋即明確說明在我國個資法下，蒐集者須承擔目標對象得以充分瞭解受告知法定資訊內容之責，以確保當事人同意的「知情性」之落實。

（四）明確性

當事人之同意須以清楚肯定的積極行為表示，否則易生當事人不知情而誤遭認定已由某種不作為而接受同意之爭議。

歐盟 GDPR 前言第 32 點第 2 段與第 3 段指出，清楚肯定之行為可包括瀏覽網站時勾選框格、使用資訊社會服務時選擇特定的技術設定，或其他清楚表示當事人接受處理其個人資料之請求的聲明或行動。至於沉默、預先勾選框格、不作為，則不構成當事人之同意。

此外，依美國加州 CCPA 第 1798.140 條第 h 項對同意之定義，游標懸停、沉默、暫停、關閉內容不構成同意，以不正方式取得之允許也不構成同意。

我國個資法第 7 條第 3 項雖有「推定同意」之規定，但應不代表個資法允許不作為的默示同意存在。個資法主管機關即曾對於某業者擬於 APP 之「在我附近的健康餐飲資訊」功能欄位畫面，提示「正在蒐集您的定位資訊」文字，並同時於畫面角落出現「□暫不提供定位資訊」一事，認為應將提示文字修正為「本服務需要蒐集您的定位資訊」，並說明如欲符合推定同意要件之「當事人未表示拒絕」，應係當事人在正面選擇同意與否之模式下進行（例如：上開畫面宜顯示

「□提供定位資訊」），否則有類似「預設同意」效果之虞；至如欲符合推定同意要件之「當事人已提供其個人資料」，應係指當事人有自行提供個人資料之積極行為（例如：自主開啟藍芽設定並選擇同步資料，並將資料傳送予業者）；倘業者預設自動上傳資料之功能，在當事人未有任何積極行為之情形下即取得個人資料，則縱使當事人未表示拒絕，仍不得視為當事人已提供其個人資料，因此應不符合推定同意之要件[305]。

（五）可撤回性

最後，對於繼續性的蒐集、處理或利用個人資料的行為，除非法律明文規定同意不得撤回，否則當蒐集者以當事人同意作為依據時，當事人既可自主表示同意，應即有權隨時（不受阻礙）撤回該同意。

通觀本報告比較研究之各國個資法，皆未見不得撤回同意之明文規範。歐盟 GDPR 第 7 條第 3 項與新加坡個人資料保護法第 16 條更明文規定當事人得撤回其同意。

對此，我國個資法目前並未明文規範當事人得撤回其同意，但解釋上不應視為當事人無此權利，否則恐將減損當事人同意的自主性。

各國個資法規關於本議題之比較表格整理如下：

表 5、各國個資目的外利用告知相關規範比較表

[305] 見國家發展委員會 107 年 11 月 11 日發法字第 1072002136 號函。

國家		權利內容	法源依據	位階
臺灣		1、 蒐集個資之同意係指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。 2、 目的外利用個資之同意係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。	個人資料保護法第 7 條	法律
歐盟		1、 同意應自願、特定、知情、明確，由個資當事人以積極行為作出。 2、 撤回同意應與給予同意同樣容易。	GDPR §§4(11), 7(3)	法律
美國	加州	1、 同意應自願、特定、知情、明確，為特定目的，並由消費者以聲明或積極行為作出。 2、 下列情形不構成有效同意： (1) 接受非專門約定個人資訊事宜之使用條款； (2) 用滑鼠游標標定、靜音、暫停或關閉特定內容； (3) 以不正方式(dark patterns)獲取當事人同意。	CCPA, amended by CPRA § 1798.140(h)	法律
	維吉尼	1、 同意應自願、特定、知情、明確，並由消費者以積極行為作出。 2、 同意得以電子文件方式作出。	CDPA §59.1-571	法律

國家	權利內容	法源依據	位階
亞州			
日本	應以合理、適當之方式取得同意。	個人資訊保護委員會指引第 2-12 節	主管機關指引
韓國	1、 個資處理者應就各同意事項分別取得個資當事人之同意。 2、 如以書面取得個資當事人之同意，應告知個資蒐集利用目的、類別等。	個人資料保護法 §22	法律
新加坡	1、 除法律明文規定無須同意之情形外，非經個資當事人同意或視為同意，組織不得蒐集、利用或揭露個人資料。 2、 當事人若未經告知個人資料蒐集、利用或揭露之目的，所給予之同意無效。 3、 組織不得： (1) 不合理地將同意作為提供產品或服務之前提條件； (2) 為獲得同意而提供不實或誤導性資訊，或採取欺騙或誤導性方式。 4、 特定情形下，如個資當事人為特定目的主動提供個人資料時，視	PDPA §§13-16	法律

國家	權利內容	法源依據	位階
	為當事人已同意。 5、 個資當事人得隨時撤回同意。		

五、修法需求分析與本節結論

由上述法規比較可知，「自主性」、「特定性」、「知情性」、「明確性」與「可撤回性」應是當事人同意應具備的普世條件。

然而，我國個資法尚未將「自主性」列為同意之要件；且個資法第7條第1項與第2項雖要求蒐集者應揭露特定資訊始可取得有效之同意（知情性），但未於法規條文中強調「特定性」要件，即未明確要求蒐集者針對不同目的應分別給予當事人表達同意與否之機會，並應就徵求同意之請求與其他內容明確區分，此或將造成蒐集者將複數目的並列揭露，徵求當事人一次性表示同意的結果。

又在「知情性」方面，個資法第8條或第9條雖要求蒐集者向當事人告知特定資訊、第7條第1項與第2項亦要求蒐集者在取得當事人同意時應以（明確）告知特定資訊為前提，但似未要求蒐集者於告知法定資訊時，其內容應特重目標對象的有效理解（此為個資法主管機關於前述函釋中所強調）[306]。

另在「明確性」部分，雖然我國個資法第7條第1項中的「所為允許」或第7條第2項中的「單獨所為」，應指當事人須有「積極行為」表示其同意，惟因個資法第7條第3項尚允許「推定同意」，其中「未表示拒絕」要件即似與前述「積極行為（表示允許）」易生混淆，主管機關尚須以函釋說明其意（例如：不得預設同意）。

且縱使當事人可任意「撤回同意」，於法理上應為有效同意的當然解釋，但因我國個資法並未明文規定（包含配套措施），因此

[306] 個資法施行細則第16條僅規定告知「得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之」，未針對內容清晰性定有規範。

實務上鮮見蒐集者向當事人提供撤回同意之方式、管道，更遑論於徵求同意時向當事人告知有權撤回同意。

考量當事人同意乃我國個資法規範蒐集、處理與利用個人資料之合法要件（之一），違反者將面臨刑事、行政或民事責任，若僅以主管機關發布指引或函釋之方式闡明前述同意要件，恐於「法律明確性」之檢視產生爭議。本報告據此認為，我國個資法宜於條文中以適當文字納入前述「自主性」、「特定性」、「知情性」、「明確性」與「可撤回性」等同意之條件，並可於施行細則對此些條件細為規範，架構有效的當事人同意法規框架。

第六節 個資衝擊影響評估

一、議題釐清

本議題源於「臺灣開放政府國家行動方案」中的承諾事項 1-3「強化數位隱私與個資保護」[307]，欲探究者為「現行個資法施行細則雖有規定得採行『個資之風險評估及管理機制』措施，惟哪些業務需進行評估及如何評估，尚不明確，是否可透過指引等方式釐清適用範圍、情形等」。對此，本議題即須針對「個資衝擊影響評估之適用情況、範圍與評估內容要件及配套措施」進行研議。

以下將從「何種情形下須執行個資衝擊影響評估」與「個資衝擊影響評估應如何執行」兩個面向分別檢視。

二、我國個人資料保護法

（一）個資衝擊影響評估執行義務

我國個資法施行細則第 12 條第 2 項第 3 款規定，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，所採取之技術上及組織上措施，得包括「個人資料之風險評估及管理機制」。據此，我國個資法上的個人資料風險評估，係對個資安全性的評估。且該評估並之執行並無強制標準，而是由個人資料蒐集、處理或利用機關考量實際狀況辦理。

中央目的事業主管機關可能對管轄範圍內之非公務機關訂有個人資料風險評估要求。例如，依《金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法》第 5 條，金融服務業者機關應依所界定之個人資料範圍及其業務涉及個人資料蒐集、處理、利用之流程，評估可能產生之個人資料風險，並根據風險評估之結果，訂定適當之管理機制。依經濟部所訂之《網際網路零售業及網際網路零售服務平台業個

[307] 臺灣開放政府國家行動方案，2021 年 4 月，頁 12-15。

人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法》第 7 條，網際網路零售業應適時並每年定期評估其因蒐集、處理或利用個人資料可能面臨的法律或其他風險，並訂定適當之管控及因應措施。

教育部訂定之《私立兒童課後照顧服務中心個人資料檔案安全維護計畫實施辦法》第 10 條、勞動部訂定之《人力仲介業個人資料檔案安全維護計畫及處理辦法》第 7 條，內政部訂定之《移民業務機構個人資料檔案安全維護管理辦法》第 7 條亦包含類似風險評估規範。

（二）個資衝擊影響評估執行方式

我國個資法施行細則第 12 條第 2 項要求公務機關於非公務機關所採取之安全維護措施，與所欲達成之個人資料保護目的間具有適當比例，此一要求亦適用於作為安全維護措施的個人資料之風險評估及管理機制。除此以外，我國個資法、個資法施行細則、中央目的事業主管機關相關規範及主管機關之見解，未見關於如何執行個人資料風險評估之具體規範。

由上述規範可知，我國個資法將個人資料風險評估作為個人資料安全維護措施之一，但對於風險評估之執行標準與方式，尚未見細部規範。

三、外國立法例

（一）歐盟 GDPR

歐盟 GDPR 在歐盟法中導入個資衝擊影響評估（DPIA）制度。GDPR 自身並未對 DPIA 進行定義，而 WP29 在其關於 DPIA 之指引中，認為 DPIA 係一種程序，該程序描述資料處理，評估處理之必要性及合比例性，評估個資處理對自然人

權利和自由產生之風險並決定因應措施，以協助管控此等風險。DPIA 係實現並證明法令遵循之工具[308]。

1、個資衝擊影響評估執行義務

GDPR 第 35 條第 1 項規定，若一項處理（特別是使用新技術的處理，且考量處理之性質、範圍、背景與目的）可能導致自然人權利和自由的高風險，則控管者應於處理之前，評估擬進行的處理作業對個人資料保護之影響[309]。WP29 認為，GDPR 採風險導向（risk-based）之方法，控管者執行 DPIA 之義務，其基礎是 GDPR 第 24 條第 1 項規定的控管者基於處理作業所涉風險之可能性和嚴重性，採取技術性與組織性措施之義務。該項所稱的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，但也可能涉及其他基本權利，如言論自由、思想自由等[310]。

關於可能導致高風險之處理，GDPR 第 35 條第 3 項包含相關舉例。下列情形下，「尤其」應執行 DPIA：(1)以自動化方式（包括剖析）對自然人個人特質進行系統性、大規模評估，且據此作出的決定將對個資當事人有法律效果或類似重大影響；(2)處理 GDPR 第 9 條規定的特種個資，或 GDPR 第 10 條規定的前科或犯罪相關個資；(3)大規模系統性監視公共區域[311]。

[308] WP29, 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 (4 October 2017) 4.

[309] 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 protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."

[310] WP29, 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 (4 October 2017) 6.

[311] EU, GDPR, §35(3), "A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions

此外，WP29在其指引中，提供了評估高風險之九項考量要素。若擬進行的處理作業符合其中兩項或更多，原則應執行 DPIA。(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」之評估；(2)具有法律效果或類似重大影響之自動化決策；(3)對當事人之系統性監控；(4)處理特種個資或高度私人性的資料；(5)從所涉人數、資料數量、持續時間等方面，大規模處理個資；(6)匹配或組合不同資料集；(7)處理弱勢當事人之資料；(8)創新利用或應用新的技術性或組織性解決方案；(9)處理自身將阻止當事人行使權利或使用服務或契約[312]。

GDPR 第 35 條第 4 項要求主管機關訂定並公布強制執行DPIA之處理作業清單[313]。若控管者擬進行的處理作業落入該清單範圍內，則必須執行 DPIA。

GDPR 第 35 條第 5 項允許主管機關訂定並公布無需執行DPIA之處理作業清單[314]。若控管者擬進行的處理作業落入該清單範圍內，則無需執行 DPIA。

此外，依GDPR第35條第10項，符合下列條件時，以會員國法律為依據的處理作業無需執行 DPIA，但會員國認為仍有必要執行 DPIA 者除外：（1）法律以會員國

are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale."

[312] WP29, 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 (4 October 2017) 9-11.

[313] EU, GDPR, §35(4), "The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68."。

[314] EU, GDPR, §35(5), "The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board."。

若處理之合法要件係「遵守法律義務」或「執行符合公益之職務或行使公權力」；（2）作為依據之會員國法律對該處理作業有相關規範；且（3）在該法律制定過程中，已就其對個資保護之影響進行評估[315]。此外，依 GDPR 第 35 條第 1 項，風險相似的數項類似處理作業得以同一份 DPIA 進行評估。據此，WP29 的指引認為，若處理之性質、範圍、背景和目的與已執行之DPIA非常相似，則可使用類似處理之 DPIA 的結果[316]。

關於已在進行中的處理作業是否需要執行 DPIA，WP29認為，若現行處理作業可能對自然人之權利和自由造成高風險；或考量處理之性質、範圍、背景和目的，處理所涉風險已發生變化，則控管者應執行 DPIA[317]。

2、 個資衝擊影響評估執行方式

依 GDPR 第 35 條第 1 項和第 10 項，及前言第 90 點和第 93 點，應於「處理前」執行 DPIA。WP29 認為，此與資料保護設計（by design）和預設（by default）原則一致。WP29 還指出，DPIA 並非一次性行為，而是一種持續進行的程序，當處理作業在動態變化時尤為如此[318]。

依GDPR第35條第2項，控管者應確保執行DPIA。WP29 的指引說明，DPIA 得由組織內部或外部其他人員

[315] EU, GDPR, §35(10), "Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities."

[316] WP29, 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 (4 October 2017) 7, 12.

[317] WP29, 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 (4 October 2017) 13-14.

[318] WP29, 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 (4 October 2017) 14.

完成，但控管者應對DPIA負最終責任。控管者若已指派個資保護官（DPO），則應於執行 DPIA 時，應尋求DPO之建議[319]。

此外，依第 28 條第 3 項第 f 款，若處理作業之全部或一部係由受託處理者實施，則受託處理者應協助控管者執行DPIA，並提供任何必要之資訊[320]。依GDPR第35條第 9 項，在不損害商業或公共利益或處理作業安全之前提下，控管者應於適當時尋求個資當事人或其代表人對處理的意見[321]。WP29的指引說明，若控管者認為不適合尋求當事人意見，或控管者的最終決定與當事人之意見不同，控管者皆應記錄相關理由[322]。

DPIA 的內容，依 GDPR 第 35 條第 7 項規定，至少應包含如下要素：(1)描述擬進行的處理作業和處理之目的；(2)評估處理之必要性及合比例性；(3)評估對當事人權利和自由之風險；(4)預計採取的因應風險和證明法遵的措施[323]。

[319] EU, GDPR, §35(2), "The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment."

[320] EU, GDPR, §28(3), "Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:… (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;…"

[321] EU, GDPR, §35(9), "9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations."

[322] WP29, 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 (4 October 2017) 15.

[323] EU, GDPR, §35(7), "The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned."

依第 35 條第 8 項，在評估處理作業之影響時，必須考量 GDPR 第 40 條規定的行為守則之遵守[324]。WP29 認為，在遵守適當行為守則的前提下，考量行為守則有利於證明已選擇或實施適當措施。

WP29 進一步認為，用以證明控管者和處理者處理作業遵守 GDPR 之認證、標章和標誌，以及具有約束力之企業守則（BCR），亦應納入考量[325]。

又依 GDPR 第 36 條第 1 項，若 DPIA 結果顯示，控管者如不採取降低風險之措施，處理將導致高風險，則控管者應於處理前諮詢監管機關[326]。依 WP29 之指引，這要求控管者面對高剩餘風險時（亦即，控管者無法採取有效措施將風險降低至可接受程度時），應諮詢監管機關[327]。GDPR 並未要求公布 DPIA，但 WP29 建議，控管者應考量至少公布部分內容，例如 DPIA 的摘要或結論[328]。

在配套措施方面，GDPR 第 35 條第 11 項規定，於必要時，至少於處理作業之風險發生變化時，控管者應執行審查，以評估處理作業是否遵循 DPIA[329]。

---

[324] EU, GDPR, §35(8), "Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment."

[325] WP29, 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 (4 October 2017) 16.

[326] EU, GDPR, §36(1), "The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk."

[327] WP29, 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 (4 October 2017) 18.

[328] WP29, 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 (4 October 2017) 18.

[329] EU, GDPR, §35(11), "Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations."

由前開規範可知，GDPR 要求控管者在擬進行的處理作業可能導致自然人權利和自由的高風險時，對該處理作業執行 DPIA。DPIA 應描述擬進行的處理作業和處理之目的；評估處理之必要性及合比例性；評估對當事人權利和自由之風險；並分析預計採取的因應風險和證明法遵的措施。若 DPIA 顯示，控管者無法採取有效措施將風險降低至可接受程度，應諮詢監管機關。

（二）美國加州 CCPA

美國加州於 2020 年 11 月公投通過 CPRA，修正 CCPA 並強化消費者個資保護，增修內容包括個資衝擊影響評估制度。

1、個資衝擊影響評估執行義務

依修正後的 CCPA 第 1798.185 條第 a 項第 15 款，若業者之消費者個人資訊處理活動，對消費者的隱私或安全構成嚴重風險，州檢察長應制定施行細則，要求業者履行下列責任：(1)實施年度資安稽核；(2)定期向加州隱私保護署提交對個人資訊處理活動之風險評估結果[330]。

據此，加州 CCPA 規定之個人衝擊影響評估，呈現為資安年度稽核和定期風險評估兩個方面。業者負有此等義務之判定標準，係處理將導致消費者隱私或安全之

[330] CCPA (as amended by CPRA) 1798.185(a), "On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas: … (15) Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to: (A) Perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent. The factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities. (B) Submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public. Nothing in this section shall require a business to divulge trade secrets."

嚴重風險。依 CCPA 第 1798.185 條第 a 項第 15 款第 A 項，判斷處理是否可能導致個人資訊嚴重風險之考量要素包括：業者業務的規模和複雜程度，以及處理活動的性質與範圍。

2、個資衝擊影響評估執行方式

依修正後的 CCPA 第 1798.185 條第 a 項第 15 款第 A 項，年度資安稽核方面，州檢察長之施行細則應規定年度資安稽核之範圍，以及確保稽核徹底性與獨立性之程序。此一規範自 2020 年 12 月生效，但截至 2021 年 11 月，加州州檢察長尚未公布相關施行細則。

依修正後的 CCPA 第 1798.185 條第 a 項第 15 款第 B 項，個人資訊處理活動之風險評估應說明否處理敏感個人資訊，識別處理對業者、消費者、其他利害關係方和一般公眾之利益，以及處理對所涉消費者權利的潛在風險，衡量利益與潛在風險，並在對消費者隱私之風險大於對消費者、業者、其他利害關係方和一般公眾之利益時，限制或禁止處理。但關於風險評估之程序與頻率等，尚待州檢察長制定相關施行細則。加州隱私保護署的 CPRA 細則公告中，包含「消費者隱私或安全之嚴重風險」之解釋、落實稽核徹底性與獨立性之措施、稽核之內容與方法、風險之評估標準等。由此觀察，CCPA 關於個資衝擊影響評估的施行細則，將由加州隱私保護署制定。

綜上所述，依修正後的 CCPA，業者之處理活動若對消費者的隱私或安全構成嚴重風險，則應執行資安年度稽核和定期風險評估，並將風險評估結果提交予加州隱私保護署。風險評估值核心目標，係識別並衡量處理所涉利益與風險，

並在風險大於利益時，禁止或限制處理。至於資安稽核與風險評估之細部規範，則尚待權責機關訂定。

（三）美國維吉尼亞州 CDPA

1、個資衝擊影響評估執行義務

美國維吉尼亞州 CDPA 第 59.1-576 條係關於「資料保護評估」之規範。依該條第 A 項，控管者應就下列個人資料處理活動執行並記錄資料保護評估：(1)為精準廣告目的處理個人資料；(2)販售個人資料；(3)為剖析目的處理個人資料，且可合理預見該處理存在如下風險之一：對消費者之不公正或欺騙性對待，或違法之差別影響（disparate impact）；對消費者財產、身體或名譽之損害；以實體或其他形式打擾消費者私密空間或私人事務，且依一般人標準已構成侵擾；對消費者的其他重大損害；(4)處理敏感資料；和(5)任何對消費者有較高風險（heightened risk）之個人資料處理活動[331]。

此外，依 CDPA 第 59.1-576 條第 E 項，控管者依其他法令執行之資料保護評估，若與 CDPA 之範圍與效果相當，則可視為已遵守 CDPA 之資料保護評估要求[332]。依同條第 F 項，資料保護評估義務僅適用於該法生效後（2023 年 1 月 1 日）啟動的處理活動，並不溯及既往[333]。

[331] Virginia, CDPA, §59.1-576(A), "A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data: 1. The processing of personal data for purposes of targeted advertising; 2. The sale of personal data; 3. The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers; 4. The processing of sensitive data; and 5. Any processing activities involving personal data that present a heightened risk of harm to consumers."

[332] Virginia, CDPA, §59.1-576(E), "Data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may comply under this section if the assessments have a reasonably comparable scope and effect."

[333] Virginia, CDPA, §59.1-576(F), "Data protection assessment requirements shall apply to processing activities created or generated after January 1, 2023, and are not retroactive."

2、個資衝擊影響評估執行方式

依維吉尼亞州 CDPA 第 59.1-576 條第 B 項規定，資料影響評估的內容應識別處理活動可能為控管者、消費者、其他利害關係方和一般公眾帶來的直接或間接利益，以及處理對所涉消費者之權利可能造成的潛在風險（考量控管者可採取的風險減低措施之效果），並衡量前述利益與風險。此外，資料影響評估還應考量：對去識別化資料之使用，消費者的合理期待，處理活動的背景，以及控管者與處理所涉消費者間的關係[334]。

依維吉尼亞州 CDPA 第 59.1-576 條第 C 項，州檢察長得要求控管者提供資料影響評估結果，並據以評估控管者是否遵守 CDPA 第 59.1-574 條所定資料保護和透明化義務。資料影響評估結果應予保密，不適用依政府資訊公開法規之民眾查閱及複製規範[335]。

此外，依維吉尼亞州 CDPA 第 59.1-576 條第 C 項，單一資料保護評估可涵蓋多項類似資料處理活動。

綜上所述，維吉尼亞州 CDPA 要求控管者的處理活動涉及較高風險時，對處理活動執行資料保護評估。該法明文列舉，精準廣告、販售個人資料、可能對消費者有重大損害之

[334] Virginia, CDPA, §59.1-576(B), "Data protection assessments conducted pursuant to subsection A shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into this assessment by the controller."

[335] Virginia, CDPA, §59.1-576(C), "The Attorney General may request, pursuant to a civil investigative demand, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in § 59.1-574. Data protection assessments shall be confidential and exempt from public inspection and copying under the Virginia Freedom of Information Act (§ 2.2-3700 et seq.). The disclosure of a data protection assessment pursuant to a request from the Attorney General shall not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment."

剖析、涉及敏感資料之處理活動，強制要求執行資料保護評估。風險評估值核心目標，係識別並衡量處理所涉利益與風險。州檢察長得要求控管者提交風險評估結果，但應對該結果予以保密。

（四）日本個人資訊保護法

日本個人資訊保護法並未針對個人資料制定普遍適用之個資衝擊影響評估制度。該法配合數位社會整備法修正後，亦未引入普遍性個資衝擊影響評估制度。

（五）日本個人編號使用法

雖然日本行政機關個人資訊保護法並未針對行政機關個人資料制定普遍適用之個資衝擊影響評估制度。該法配合數位社會整備法修正後，亦未針對行政機關設置普遍性個資衝擊影響評估義務。但個人編號使用法訂有「特定個人資訊」保護評估制度，拘束行政機關。

1、個資衝擊影響評估執行義務

依個人編號使用法第 28 條，若行政機關首長擬保有「特定個人資訊」檔案（行政機關現任及曾任職員之人事、薪酬、福利紀錄，以及個人資訊保護委員會規則規定之其他資料除外），則應在保有之前，依個人資訊保護委員會規則評估相關事項，將評估結果作成書面報告予以公開，並就該評估報告徵求一般民眾之意見。若該特定個人資訊檔案發生個人資訊保護委員會規則規定之重大變化，亦應執行評估[336]。

[336] 日本，番号利用法，§28(1)，「行政機関の長等は、特定個人情報ファイル（専ら当該行政機関の長等の職員又は職員であった者の人事、給与又は福利厚生に関する事項を記録するものその他の個人情報保護委員会規則で定めるものを除く。以下この条において同じ。）を保有しようとするときは、当該特定個人情報ファイルを保有する前に、個人情報保護委員会規則で定めるところにより、次に掲げる事項を評価した結果を記載した書面（以下この条において「評価書」という。）を公示し、広く国民の意見を求めるものとする。当該

行政機關首長應依個人資訊保護委員會規則考量民眾對評估報告提出之意見，對評價報告加以必要修改，並就該評價報告所涉特定個人資訊檔案處理作業，請求個人資訊保護委員會批准[337]。個人資訊保護委員會依法審查後，如認為該處理作業符合相關指引，則應予以批准[338]。

個人資訊保護委員會批准後，行政機關首長應儘速將評估報告公開[339]。公開評估報告者，視為已符合行政機關個人資訊保護法第 10 條第 1 項之保有個人資訊檔案事前告知要求[340]。

2、個資衝擊影響評估執行方式

依個人編號使用法第 28 條第 1 項，特定個人資訊保護評估的內容包括：(1)該特定個人資料檔案處理作業者數目；(2)該特定個人資料檔案所記錄之特定個人資料數

特定個人情報ファイルについて、個人情報保護委員会規則で定める重要な変更を加えようとするときも、同様とする。一　特定個人情報ファイルを取り扱う事務に従事する者の数。二　特定個人情報ファイルに記録されることとなる特定個人情報の量。三　行政機関の長等における過去の個人情報ファイルの取扱いの状況。四　特定個人情報ファイルを取り扱う事務の概要。五　特定個人情報ファイルを取り扱うために使用する電子情報処理組織の仕組み及び電子計算機処理等（電子計算機処理（電子計算機を使用して行われる情報の入力、蓄積、編集、加工、修正、更新、検索、消去、出力又はこれらに類する処理をいう。）その他これに伴う政令で定める措置をいう。第三十八条の三及び第四十五条の二第一項において同じ。）の方式。六　特定個人情報ファイルに記録された特定個人情報を保護するための措置。七　前各号に掲げるもののほか、個人情報保護委員会規則で定める事項。」。

[337] 日本，番号利用法，§28(2)，「前項前段の場合において、行政機関の長等は、個人情報保護委員会規則で定めるところにより、同項前段の規定により得られた意見を十分考慮した上で評価書に必要な見直しを行った後に、当該評価書に記載された特定個人情報ファイルの取扱いについて委員会の承認を受けるものとする。当該特定個人情報ファイルについて、個人情報保護委員会規則で定める重要な変更を加えようとするときも、同様とする。」。

[338] 日本，番号利用法，§28(3)，「委員会は、評価書の内容、第三十五条第一項の規定により得た情報その他の情報から判断して、当該評価書に記載された特定個人情報ファイルの取扱いが指針に適合していると認められる場合でなければ、前項の承認をしてはならない。」。

[339] 日本，番号利用法，§28(4)，「行政機関の長等は、第二項の規定により評価書について承認を受けたときは、速やかに当該評価書を公表するものとする。」。

[340] 日本，番号利用法，§28(5)，「前項の規定により評価書が公表されたときは、第三十条第一項の規定により読み替えて適用する行政機関個人情報保護法第十条第一項の規定による通知があったものとみなす。」。

量；(3)行政機關首長等處理特定個人資料檔案之歷史狀況；(4)特定個人資料檔案處理作業概況；(5)特定個人資料檔案時使用之電子資訊處理系統和電子資訊處理方法等；(6)特定個人資料檔案中所含特定個人資料之保護措施；(7)個人資訊保護委員會規則規定之其他事項。

日本個人資訊保護委員會訂定「特定個人資訊保護評估規則」[341]和「特定個人資訊保護評估指引」[342]，就特定個人資訊保護評估之內容作出細部規範，以所涉個資當事人數目、特定個人資訊處理者數目，以及是否曾發生特定個人資訊相關之重大事故為基準，區分不同評估作業流程。概言之，擬保有特定個人資訊之行政機關，原則皆應先執行「基礎項目評估」。完成基礎項目評估後，視所涉個資當事人數目、特定個人資訊處理者數目是否已達相應標準，和（或）過去一年內是否曾發生重大事故，可能需執行「重點項目評估」或「全項目評估」。由此，日本特定個人資訊保護評估係採層級化執行模式。

綜上所述，日本行政機關之個資衝擊影響評估義務，以涉及特定個人資訊檔案（即包含個人編號之個人資訊檔案）為限。特定個人資訊檔案保護評估之結果報告須公開徵求意見，且處理作業須經個人資訊保護委員會批准。

（六）韓國個人資料保護法

1、個資衝擊影響評估執行義務

[341] 特定個人情報保護評価に関する規則（平成二十六年特定個人情報保護委員会規則第一号，令和三年個人情報保護委員会規則第三号による改正）。

[342] 特定個人情報保護評価指針（平成二十六年特定個人情報保護委員会告示第四号，令和３年個人情報保護委員会告示第１号による改正）。

依韓國個人資料保護法第 33 條第 1 項，運用大統領令規定之個人資料檔案，且致使當事人個人資料面臨侵害風險時，公務機關首長應執行影響評估（以下稱隱私影響評估），以分析風險因素並提出改善措施[343]。

依個人資料保護法施行令第 35 條，所謂「大統領令」規定之個人資料檔案，係指得以電子方式處理，且符合下列情形之一的個人資料檔案：(1)擬製作、運用或修改，且包含 5 萬名或以上當事人敏感資料或固有識別性資料；(2)已製作並運用，將與擬製作並於公務機關內部或外部運用的其他個人資料檔案相比對，且經比對後將包含 50 萬名或以上當事人個人資料；(3)擬製作、運用或修改，且包含 100 萬名或以上當事人個人資料；(4)該檔案之運用系統（包括資料檢索系統），將於隱私影響評估後予以變更；此時，隱私影響評估之對象以變更部分為限[344]。

---

[343] 한국，개인정보보호법，§33(1)，“공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일 의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 "영향평가"라 한다)를 하고 그 결과를 보호위원회에 제출하여야 한다. 이 경우 공공 기관의 장은 영향평가를 보호위원회가 지정하는 기관(이하 "평가기관" 이라 한다) 중에서 의뢰하여야 한다.”

[344] 한국，개인정보보호법시행령，§35，“법 제 33 조제 1 항에서 “대통령령으로 정하는 기준에 해당하는 개인정보파일” 이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다. 1. 구축・운용 또는 변경하려는 개인정보파일로서 5 만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일. 2. 구축・운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축・운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50 만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일. 3. 구축・운용 또는 변경하려는 개인정보파일로서 100 만명 이상의 정보주체에 관한 개인정보파일. 4. 법 제 33 조제 1 항에 따른 개인정보 영향평가(이하 “영향평가” 라 한다)를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다.”

依個人資料保護法第 33 條第 8 項，個人資料檔案之運用致使當事人個人資料面臨侵害風險，公務機關以外的個人資料處理者應積極執行隱私影響評估[345]。

2、個資衝擊影響評估執行方式

依韓國個人資料保護法第 33 條第 2 項，隱私影響評估應考量如下內容：(1)所處理之個人資料數量；(2)個人資料是否會提供予第三方；(3)損害個資當事人權利之可能性及風險程度；(4)大統領令規定之其他事項[346]。依個人資料保護法施行令第 36 條，隱私影響評估還應包含個人資料之保存期間；以及是否處理敏感資料或固有識別性資料[347]。

依韓國個人資料保護法第 33 條第 1 項，隱私影響評估應由韓國個人資料保護委員會指定機構（以下稱隱私評估機構）實施。依同法第 60 條，執行隱私評估之人員應對評估所涉機密資訊保密。個人資料保護法施行令第 37 條則規定前述隱私評估機構之資格要件、申請程序與管理制度。

依個人資料保護法施行令第 38 條，隱私影響評估之基準包括：(1)個人資料檔案所含個人資料之類別和性質，個人當事人數量，以及發生個人資料損害之風險；(2)依個人資料保護法採取之安全措施，以及發生個人資料損

345 한국，개인정보보호법，§33(8)，“공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보 주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 한다.”

346 한국，개인정보보호법，§33(2)，“영향평가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다. 1. 처리하는 개인정보의 수. 2. 개인정보의 제 3 자 제공 여부. 3. 정보주체의 권리를 해할 가능성 및 그 위험 정도. 4. 그 밖에 대통령령으로 정한 사항.

347 한국，개인정보보호법시행령，§36，“법 제 33 조제 2 항제 4 호에서 “대통령령으로 정한 사항”이란 다음 각 호의 사항을 말한다. 1. 민감정보 또는 고유식별정보의 처리 여부. 2. 개인정보 보유기간.”

害之風險；(3)個人資料損害風險之因應措施；(4)其他法定必要措施，或影響履行責任的其他因素。隱私評估機構收到隱私評估申請後，應依據前開基準分析並評估個人資料檔案運用所涉個人資料損害風險，撰寫隱私影響評估報告，並將該報告提交予公務機關首長。隱私影響報告應說明運用個人資料檔案之業務概要和運用目的，概述所評估之個人資料檔案，分析並評估個人資料檔案運用所涉個人資料損害風險，提出待改善之處，說明隱私影響評估所需人力資源與成本[348]。

最後，依個人資料保護法第 33 條第 1 項和個人資料保護法施行令第 38 條第 2 項規定，公務機關首長應在製作、使用或變更個人資料檔案前，將隱私影響評估報告（包括待改善之處）提交予韓國個人資料保護委員會。依個人資料保護法第 33 條第 3 項，韓國個人資料保護委員會得就評估結果提出意見。依同條第 4 項，公務機關

[348] 한국，개인정보보호법시행령，§38，“① 법 제 33 조제 6 항에 따른 영향평가의 평가기준은 다음 각 호와 같다. 1. 해당 개인정보파일에 포함되는 개인정보의 종류・성질, 정보주체의 수 및 그에 따른 개인정보 침해의 가능성. 2. 법 제 24 조제 3 항, 제 25 조제 6 항 및 제 29 조에 따른 안전성 확보 조치의 수준 및 이에 따른 개인정보 침해의 가능성. 3. 개인정보 침해의 위험요인별 조치 여부. 4. 그 밖에 법 및 이 영에 따라 필요한 조치 또는 의무 위반 요소에 관한 사항.② 법 제 33 조제 1 항에 따라 영향평가를 의뢰받은 평가기관은 제 1 항의 평가기준에 따라 개인정보파일의 운용으로 인한 개인정보 침해의 위험요인을 분석・평가한 후 다음 각 호의 사항이 포함된 평가 결과를 영향평가서로 작성하여 해당 공공기관의 장에게 보내야 하며, 공공기관의 장은 제 35 조 각 호에 해당하는 개인정보파일을 구축・운용 또는 변경하기 전에 그 영향평가서를 보호위원회에 제출(영향평가서에 제 3 호에 따른 개선 필요 사항이 포함된 경우에는 그에 대한 조치 내용을 포함한다)해야 한다. 1. 개인정보파일 운용과 관련된 사업의 개요 및 개인정보파일 운용의 목적. 2. 영향평가 대상 개인정보파일의 개요. 3. 평가기준에 따른 개인정보 침해의 위험요인에 대한 분석・평가 및 개선이 필요한 사항. 4. 영향평가 수행 인력 및 비용.③ 보호위원회는 법 및 이 영에서 정한 사항 외에 평가기관의 지정 및 영향평가의 절차 등에 관한 세부 기준을 정하여 고시할 수 있다.”

首長將經評估之個人資料檔案依同法第 32 條進行備案時，應附上評估結果[349]。

由前述規範可知，依韓國個人資料保護法規定，公務機關運用特定性質、規模之個人資料檔案前，強制執行隱私影響評估。隱私影響評估應由隱私評估機構執行，影響評估報告應提交予個人資料保護委員會，並在法定系統備案。

對於非屬公務機關之個人資料處理者，韓國個人資料保護法鼓勵執行隱私保護影響評估，但並無強制要求。

（七）新加坡個人資料保護法

1、 個資衝擊影響評估執行義務

新加坡 2020 年修正個人資料保護法，新增關於「經通知視為同意」（deemed consent by notification）、以及依據正當利益蒐集、利用和揭露個人資料之規範。此等規範要求執行個資衝擊影響評估。

依新加坡 PDPA 第 15A 條第 4 項第 a 款要求，組織如擬依據「經通知視為同意」規範蒐集、利用或揭露個人資料，須在蒐集、利用或揭露個人資料前，對擬進行的個人資料蒐集、利用或揭露行為執行評估，以確認該行為不致對當事人產生不利影響。

[349] 한국，개인정보보호법，§33，“① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 “영향평가” 라 한다)를 하고 그 결과를 보호위원회에 제출하여야 한다. 이 경우 공공기관의 장은 영향평가를 보호위원회가 지정하는 기관(이하 “평가기관” 이라 한다) 중에서 의뢰하여야 한다.… ③ 보호위원회는 제 1 항에 따라 제출받은 영향평가 결과에 대하여 의견을 제시할 수 있다. ④ 공공기관의 장은 제 1 항에 따라 영향평가를 한 개인정보파일을 제 32 조제 1 항에 따라 등록할 때에는 영향평가 결과를 함께 첨부하여야 한다.”

又新加坡 PDPA 附表 1 規範無需當事人同意即可蒐集、利用和揭露個人資料之條件。依附表 1 第 3 部分第 1 條第 1 項，組織得基於自身或他人之正當利益蒐集、利用或揭露個人資料，但所依據之正當利益，須超越對當事人之不利影響。依同條第 2 項第 1 款，組織須在蒐集、利用或揭露個人資料前執行評估，以確定是否符合前開條件[350]。

2、 個資衝擊影響評估執行方式

新加坡個人資料保護法第 15A 條第 5 項和附表 1 第 3 部分第 1 條第 3 項規定，執行評估時，組織應：(1)基於相關目的，識別擬進行的蒐集、利用或揭露行為可能對當事人造成之不利影響；(2)識別並執行合理因應措施，以消除不利影響、降低不利影響之發生機率，或減輕不利影響；且(3)遵守其他法定要求。

依新加坡 2021 年個人資料保護細則（Personal Data Protection Regulations 2021）第 14 條，若「經通知視為同意」之評估結果顯示，擬進行的個人資料蒐集、利用或揭露不致對當事人產生不利影響，則該評估結果應說明下列內容：(1)擬蒐集、利用或揭露之個人資訊類別和數量；(2)蒐集、利用或揭露個人資訊之目的；(3)蒐集、利用或揭露個人資訊之方法；(4)就擬進行之個人資料蒐集、利用或揭露行為，通知當事人的方式；(5)當事人不同意擬進行之個人資料蒐集、利用或揭露行為時，通知組織

[350] Singapore, PDPA 1st Schedule Part 3, §1, "(1) Subject to sub-paragraphs (2), (3) and (4) —(a) the collection, use or disclosure (as the case may be) of personal data about an individual is in the legitimate interests of the organisation or another person; and (b) the legitimate interests of the organisation or other person outweigh any adverse effect on the individual. (2)For the purposes of sub-paragraph (1), the organisation must —(a) conduct an assessment, before collecting, using or disclosing the personal data (as the case may be), to determine whether sub-paragraph (1) is satisfied; and (b) provide the individual with reasonable access to information about the organisation's collection, use or disclosure of personal data (as the case may be) in accordance with sub-paragraph (1)."

的期間與方式，以及確定該通知期間與方式之理由。組織在基於「經通知視為同意」蒐集、利用或揭露該個人資料期間，須保留評估結果書面紀錄[351]。

依新加坡 2021 年個人資料保護細則第 15 條，「正當利益」所要求之評估，應包含如下內容：(1)說明擬蒐集、利用或揭露之個人資訊類別和數量，蒐集、利用或揭露個人資訊之目的，以及蒐集、利用或揭露個人資訊之方法；(2)識別執行因應措施後，對當事人之剩餘風險；(3)識別作為蒐集、利用或揭露個人資料正當性理由的正當利益；(4)若所涉正當利益為他人之正當利益，說明該他人之姓名或其他特徵；(5)說明該正當利益超越對當事人不利影響之原因。組織在基於正當利益蒐集、利用或揭露該個人資料期間，須保留評估結果書面紀錄[352]。

[351] Singapore, Personal Data Protection Regulations 2021, §14, "… (2) An assessment mentioned in section 15A(4)(a) of the Act to determine that a proposed collection, use or disclosure of personal data by an organisation is not likely to have an adverse effect on an individual must specify all of the following information: (a) the types and volume of personal data to be collected, used or disclosed, as the case may be; (b) the purpose or purposes for which the personal data will be collected, used or disclosed, as the case may be; (c) the method or methods by which the personal data will be collected, used or disclosed, as the case may be; (d) the mode by which the individual will be notified of the organisation's proposed collection, use or disclosure (as the case may be) of the individual's personal data; (e) the period within which, and the mode by which, the individual may notify the organisation that the individual does not consent to the organisation's proposed collection, use or disclosure (as the case may be) of the individual's personal data; (f) the rationale for the period and mode mentioned in sub‑paragraph (e). (3) The organisation must retain a copy of its assessment mentioned in section 15A(4)(a) of the Act relating to the collection, use or disclosure of personal data about an individual throughout the period that the organisation collects, uses or discloses personal data about the individual under section 15A(2) of the Act."

[352] Singapore, Personal Data Protection Regulations 2021, §15, "…(2) An assessment mentioned in paragraph 1(2)(a) of Part 3 of the First Schedule to the Act in respect of the intended collection, use or disclosure of personal data must —(a) specify —(i) the types and volume of personal data to be collected, used or disclosed, as the case may be; (ii) the purpose or purposes for which the personal data will be collected, used or disclosed, as the case may be; and (iii) the method or methods by which the personal data will be collected, used or disclosed, as the case may be; (b) identify any residual adverse effect on any individual after implementing any reasonable measures mentioned in paragraph 1(3)(b) of Part 3 of the First Schedule to the Act; (c) identify the legitimate interests that justify the collection, use or disclosure (as the case may be) by the organisation of personal data about the individual; (d) where the legitimate interests identified under sub‑paragraph (c) relate to a person other than the organisation, identify that other person by name or description; and (e) set out the reasons for the organisation's conclusion that the legitimate interests identified under sub‑paragraph (c) outweigh any adverse effect on the individual. (3) The organisation must retain a copy of the assessment it conducted in accordance with paragraph 1(2)(a) of Part 3 of the First Schedule to the Act relating to the collection, use or disclosure of personal data about an individual throughout the period that the organisation collects, uses or discloses personal data about the individual under paragraph 1(1) of Part 3 of the First Schedule to the Act."

由前述規範可知，依新加坡 PDPA，若組織蒐集、利用或揭露個人資料的依據是「經通知視為同意」或「正當利益」，則應就蒐集、利用或揭露個人資料對當事人可能造成之不利影響進行評估。在蒐集、利用或揭露相關個人資料期間，組織應保留評估結果之書面紀錄。

四、法規比較

自上述比較法觀察，不同國家之個資衝擊影響評估制度在制度定位、制度內容等方面，可能有較大差異，以下將分別比較。

（一）個資衝擊影響評估制度定位

綜觀前述立法例之相關規範，可知上開各國個資衝擊影響評估皆為風險導向之制度。根據個資衝擊影響評估所欲管控之風險類別與特徵，可將我國及國外之個資衝擊影響評估制度大致分為「因應安全風險」與「因應當事人權益風險」兩類。先予敘明者係，此兩分類並非彼此互斥，蓋資料安全風險乃引發當事人權益風險之因素之一，故對當事人權益風險之評估與因應，其範圍自包含對資料安全風險。兩類個資衝擊影響評估詳述如下：

1、因應安全風險之個資衝擊影響評估

此類個資衝擊影響評估制度之目標，係瞭解、防範、管理並因應個人資料可能面臨之竊取、洩漏、竄改或其他安全侵害。我國[353]、日本和韓國的個資衝擊影響評估制度皆屬此類。

日本個人編號使用法所定特定個人資訊保護評估之內容，除所涉特定個人資訊之數量、處理背景、處理方

[353]「個人資料之風險評估及管理機制」列於我國個資法施行細則第 12 條第 2 項第 3 款，依同條第 1 項規定，屬於「為防止個人資料被竊取、竄改、毀損、滅失或洩漏」的技術上措施之一，係以個人資料安全風險為考量。

法等外，還包括個人資料之保護措施。韓國個人資料保護法所規定之影響評估，背景是個人資料面臨侵害風險，主要評估基準包括發生個人資料損害之風險、依法採取之安全措施、個人資料損害風險之因應措施等。

由以上可知，我國、日本及韓國個資法律上的個資衝擊影響評估，其制度定位是資料安全風險之防範與因應。

2、 因應當事人權益風險之個資衝擊影響評估

此類個資衝擊影響評估制度之目標，係瞭解個人資料之蒐集、處理、利用、揭露等，對當事人權益可能造成之損害，並防範、減緩或以其他方式因應該損害。

歐盟、美國加州、美國維吉尼亞州、新加坡的強制性個資衝擊影響評估制度皆屬此類。歐盟 GDPR 所要求之 DPIA，其核心目的是評估處理作業可能導致自然人權利和自由的高風險，以及因應措施之效用；且作為評估對象的權利與自由，未必以資料保護和隱私權利為限。美國加州 CCPA 所規定的個人資訊處理活動之風險評估，係為因應對消費者的隱私或安全之嚴重風險，且其評估將衡量處理活動所生利益與所致風險。美國維吉尼亞州 CDPA 所規範之資料保護評估，評估對象為對消費者有較高風險之各類個人資料處理活動，且其評估亦衡量處理活動所生利益與所致風險。新加坡 PDPA 強制要求的個人資料蒐集、利用或揭露行為評估，目的是判斷推定當事人同意或未經當事人同意而蒐集、利用或揭露個人資料時，其行為不致對當事人產生不利影響，或已符合法定利益衡平要求。

由以上可知，歐盟、美國加州、美國維吉尼亞州、新加坡個資法律上的個資衝擊影響評估，其制度定位是當事人權益風險之防範與因應。

（二）個資衝擊影響評估制度內容

除我國外，國外各國之個資衝擊影響評估制度，無論其制度定位如何，皆以「嚴重風險」為前提。其中，歐盟GDPR、美國加州 CCPA、韓國個人資料保護法之相關條文，均包含高風險或嚴重侵害之明文。而日本與新加坡則是將該制度運用於高風險之情境。依日本個資法律，個資衝擊影響評估制度僅適用於包含個人編號（係身分證號轉換而得）之個人資訊。

而新加坡之強制性個資衝擊影響評估制度，係伴隨推定當事人同意、無需當事人同意而利用個人資料制度而增設。此等情形下，由於未實際取得當事人知情明確同意，且不具備明確法律規範等正當性理由，當事人權益受損之風險相應升高。

無論是因應安全風險或是因應當事人權益風險，個資衝擊影響評估皆包括個資蒐集處理利用作業概述、風險識別、風險因應三個基本階段。但因所涉風險不同，風險之識別與因應方式有異。較之於針對安全風險之評估，針對權益風險之評估可能涉及不同方面利益之衡量與比較。

各國個資法規關於本議題之比較表格整理如下：

表 6、各國個資衝擊影響評估相關規範比較表

國家	權利內容	法源依據	位階
臺灣	資料蒐集、處理或利用機關之安全維護措施，得包括「個人資料之風險評估及管理機制」。	個人資料保護法施行細	主管機關命令

國家		權利內容	法源依據	位階
			則第 12 條第 3 款	
歐盟		1、若處理個資（特別是使用新技術之處理）可能造成個資當事人權利及自由之高風險時，控管者應於處理前，對該處理行為執行個資衝擊影響評估。 2、下列情形尤應執行個資衝擊影響評估： (1) 以自動化方式對自然人個人特質進行系統性、大規模評估，且據此作出的決定將對個資當事人有法律或類似重大效果； (2) 處理敏感個資或前科犯罪相關個資； (3) 大規模系統性監視公共區域。	GDPR§35	法律
美國	加州	若業者之個人資訊處理活動可能對消費者造成嚴重風險，業者應： 1、每年實施資安查核； 2、定期向加州隱私保護署提交風險評估結果。	CCPA, amended by CPRA § 1798.185 (a)(15)	法律
	維吉尼亞州	控管者於下列情形，須執行個資衝擊影響評估： 1、為精準廣告目的處理個人資料； 2、販售個人資料； 3、為剖析目的處理個資資料，且符合法定條件；	CDPA §59.1-576	法律

國家	權利內容	法源依據	位階
	4、處理敏感資料； 5、對消費者有較高風險之個資處理。		
日本	日本個資法規並無個資衝擊影響評估相關規範	-	-
韓國	1、公共機關首長依總統令，使用個人資料檔案而致個資有侵害之虞時，應執行影響評價，以分析風險並提出因應措施。 2、影響評價應由個資保護主管機關指定機構執行，評價結果應提交予主管機關，由主管機關提出評價意見。	個人資料保護法§33	法律
新加坡	在「經通知視為同意（deemed consent by notification）」或「正當利益」之情形，組織於蒐集、利用或揭露個人資料前，須評估該等行為不致對個資當事人產生不利影響。該評估須分析可能產生的不利影響，並提出防範、消除或減輕不利影響之措施。	PDPA §15A、§15	法律

五、修法需求分析與本節結論

如前文所述，我國個資法將個人資料風險評估作為資料安全維護措施之一，但對於風險評估之執行標準與方式，尚未見細部規範。而觀察國外立法例，因應安全風險與因應當事人權益風險之個資衝擊影響評估對基本步驟相似，但目的與效果迥然相異[354]。

[354] 張陳弘（2021），〈科技智慧防疫與個人資料保護：陌生但關鍵的資料保護影響評估程序〉，《臺大法學論叢》，50 卷 2 期，頁 351。

從強化當事人資訊隱私權保障之角度，我國似可考慮調整並擴充個資衝擊影響評估制度，由對資料安全風險之評估轉型為對當事人權益風險之評估。惟此一轉變必然將增加公務及非公務機關個資保護法令遵循之難度與成本。為減緩對我國社會及行業之衝擊，並考量個人資料蒐集處理利用所涉之風險，我國個資法似可考慮將強制性當事人權益風險評估之適用範圍限定於公務機關及主管機關指定之個資保護風險較高之行業。

參考比較法上相關規範，當事人權益風險評估應以客觀標準為之，其內容應包括對於蒐集處理利用目的及預期利益之概述、當事人權益風險之識別、蒐集處理利用作業必要性與合比例性之評估，以及風險防範與減緩措施之規劃。

惟如主管機關在擬訂個資法修正草案過程中，經評估認為當事人權益風險評估模式對於我國社會與行業之衝擊仍嫌過重，亦可思考維持現行資料安全評估模式，並參酌韓國個人資料保護法相關內容，在我國個資法施行細則中，增訂定安全風險類別、適用範圍、評估標準、安全考量事項、具體步驟、評估結果處理方式等細部規範。

第七節 個資保護官（DPO）

一、議題釐清

本議題源於「國家人權行動計畫（初稿）」第四章第五節第一目之人權議題「建立獨立的隱私專責機關及隱私保護專員（個資保護官）機制」[355]。由於個資法第 18 條雖要求公務機關指定專人辦理個人資料檔案安全維護事項、個資法施行細則第 12 條第 2 項亦將「配置管理之人員及相當資源」列為公務機關及非公務機關得採行之安全維護措施之一，但前述「專人」或「管理之人員」之職責為何尚不明確，可否兼任其他事務、其職責與執行職務配套措施如何等問題，亦屬未定。

對此，本議題即區分「何種情形下須指派個資保護官」與「DPO 之職責與執行職務配套措施」兩面向，針對「公務機關及非公務機關設置個資保護官之必要性、設置條件及相關配套措施」進行研議。

二、我國個人資料保護法

（一）指派個資保護官

我國個資法第 18 條規定，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。個資法施行細則第 25 條規定，所謂「專人」，係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。據此，我國個資法要求公務機關指定專人負責個人資料檔案之安全維護，對非公務機關，則未有此方面之強制性要求。

中央目的事業主管機關得依個資法第 27 條制定管理辦法，要求非公務機關指定專人負責個人資料檔案安全維護事務。例如，依教育部所訂私立兒童課後照顧服務中心個人資料檔

[355] 國家人權行動計畫（初稿）（1091029 公聽會版本），2020 年 10 月，頁 61。

案安全維護計畫實施辦法第 7 條，課照中心應指定「專責人員」，負責規劃、訂定、修正、執行安全維護計畫及業務終止後個人資料處理方法及其他相關事項，並定期向負責人提出報告。依勞動部所訂人力仲介業個人資料檔案安全維護計畫及處理辦法第 4 條，人力仲介業就個人資料檔案安全維護管理，應「指定專人或建立專責組織」負責，並配置相當資源。

（二）個資保護官職責及執行職務配套措施

如前所述，我國個資法第 18 條要求保有個人資料檔案之公務機關指定專人，負責「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」。而非公務機關依中央目的事業主管機關要求，指定之專人或專責組織，職責在於訂定執行個人資料檔案安全維護計畫、辦理個人資料檔案安全維護管理等。

個資法施行細則第 12 條指出，所謂「安全維護事項」，係指為公務機關或非公務機關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，得包括配置管理之人員及相當資源、界定個人資料之範圍、個人資料之風險評估及管理機制、事故之預防、通報及應變機制、個人資料蒐集、處理及利用之內部管理程序、資料安全管理及人員管理、認知宣導及教育訓練、設備安全管理、資料安全稽核機制、使用紀錄、軌跡資料及證據保存，以及個人資料安全維護之整體持續改善。據此，公務或非公務機關所指定之專人，應負責上開事項。

關於指定專人之執行職務配套措施，依個資法施行細則第 25 條，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。

總結前開規範可知，我國個資法要求保有個人資料檔案之公務機關指定專人負責個人資料之安全維護事項，並向該專人提供相關專業之教育訓練。非公務機關依其中央目的事業主管機關訂定之管理辦法，可能須指派專人負責訂定執行個人資料檔案安全維護計畫、辦理個人資料檔案安全維護管理等。

三、外國立法例

（一）歐盟 GDPR

1、指派個資保護官

GDPR 在歐盟法導入個資保護官（DPO）制度。GDPR 第 37 條第 1 項要求在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，但法院行使司法權者除外；(2)控管者或處理用者之核心業務，包含需大規模、經常性且系統性監控當事人之處理作業；或(3)控管者或處理者之核心業務，包含大規模處理特種個資或與前科及犯罪相關之個人資料[356]。除前述三項條件外，依第 37 條第 4 項，歐盟或會員國法律亦得規定強制指派 DPO 之其他情形[357]。

WP29 提醒，GDPR 關於強制指派 DPO 之規範，對於控管者或受託處理者均有適用，且兩者指派 DPO 之義務應獨立判斷[358]。易言之，控管者與受託處理者應分別分析是否符合 GDPR 之強制指派 DPO 標準，一方須指派

[356] 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."

[357] EU, GDPR, §37(4), "In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors."

[358] WP29, Guidelines on Data Protection Officers ('DPOs') (5 April 2017) 9.

DPO，並不必然意味著另一方也須指派 DPO。不具備前述強制指派情形之控管者或受託處理者，得自願指派 DPO。自願指派之 DPO，亦適用 GDPR 關於 DPO 指派、職位和職責之相關規定[359]。

GDPR 第 37 條第 2 項允許企業集團僅指派一名 DPO，但要求「各據點皆易於聯繫」該 DPO[360]。依同條第 3 項，數個公務機關或機構於衡量其組織架構及規模後，亦可指派單一 DPO[361]。

第 37 條第 5 項規定指派 DPO 應以其專業能力為基礎，尤其對資料保護法規與實務之專業知識，及確實達成第 39 條所述職責之能力[362]。前言第 97 點則敘明，必要之專業知識程度應視所執行之資料處理作業，及所處理的個人資料所需之保護措施而定。

第 37 條第 6 項規定，DPO 得由控管者或受託處理者之職員充任，亦可基於服務契約由外部人員充任[363]。WP29 指出，若由控管者/受託處理者與外部組織達成 DPO 服務契約，則該組織內履行 DPO 職責的個人皆應符合 GDPR 關於 DPO 之規範[364]。

GDPR 第 37 條第 7 項要求控管者或處理者應公布 DPO 之聯絡資訊，並將 DPO 之聯絡資訊提供予相關監管

[359] WP29, Guidelines on Data Protection Officers (‘DPOs’) (5 April 2017) 5.
[360] EU, GDPR, §37(2), “A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.”
[361] EU, GDPR, §37(3), “Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.”
[362] EU, GDPR, §37(5), “The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.”
[363] 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.”
[364] WP29, Guidelines on Data Protection Officers (‘DPOs’) (5 April 2017), 12.

機關[365]。依第 38 條第 4 項，當事人得聯絡 DPO，提出與個資處理相關之一切事項，或行使其資料權利[366]。

2、 個資保護官職責及執行職務配套措施

依 GDPR 第 39 條第 1 項，DPO 應至少履行如下職責：(1)向控管者或處理者及其員工提供個資法遵資訊與建議；(2)監督對 GDPR、會員國資料保護法規、控管者或處理者個資保護政策、相關稽核之遵循狀況；(3)於接到請求時，就 DPIA 提供建議並監督 DPIA 之執行；(4)與主管機關合作；(5)於事前諮詢主管機關時，擔任控管者/處理者之聯絡窗口，並就其他事項提供諮詢[367]。

依同條第 2 項，DPO 履行其職責時，應基於處理之本質、範圍、背景與目的，適當考量處理之風險[368]。依第 38 條第 5 項，DPO 就其任務之執行情形應予保密[369]。

依 GDPR 第 38 條，控管者或受託處理者為 DPO 履行職責提供適當保障。控管者或處理者應確保 DPO 及時以適當方式，參與個資保護之一切事務[370]。DPO 應獨立

[365] EU, GDPR, §37(7), "The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority."

[366] EU, GDPR, §38(4), "Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation."

[367] EU, GDPR, §39(1), "The data protection officer shall have at least the following tasks: (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness raising and training of staff involved in processing operations, and the related audits; (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; (d) to cooperate with the supervisory authority; (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."

[368] EU, GDPR, §39(2), "The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing."

[369] EU, GDPR, §38(5), "The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law."

[370] 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."

履行其職責（前言第 97 點），詳言之，DPO 應直接向控管者或受託處理者之最高管理層報告；控管者或受託處理者應確保 DPO「不受履行職務之指示」，且「不因履行職務而遭解僱或受處罰」[371]。若 DPO 承擔額外職責，控管者或處理者應確保其額外職責不致與 DPO 之職責有利益衝突[372]。此外，控管者或受託處理者還應提供必要資源，支援 DPO 履行其職責及維持其專業知識[373]。

綜上所述，依歐盟 GDPR，若個資處理之實施者係公務機關，或控管者或受託處理者之核心業務所涉個資處理作業，需大規模、經常性且系統性監控當事人，或大規模處理特種個資或前科/犯罪個資，則須強制指派 DPO。DPO 之職責重心在於確保資料保護與個資法規遵循。控管者或處理者應確保 DPO 獨立履行其職責，並提供履行職責之必要資源。

（二）美國聯邦法

美國聯邦法規針對特定行業，例如健康照護業、金融業等，訂有指派 DPO 要求。

依美國聯邦健康保險可攜及責任法（Health Insurance Portability and Accountability Act, HIPAA）施行規則（regulation）第 164.530 條[374]第 a 項第 1 款，適用 HIPAA 之受管轄機構（covered entity）須指派「隱私官」（privacy official），負責建置與實施該機構的政策與程序。依美國聯邦金融服務業現代化法（Gramm-Leach-Bliley Act, GLBA）施

[371] EU, GDPR, §38(3), "The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor."

[372] 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."

[373] EU, GDPR, §38(2), "The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge."

[374] 45 CFR 164.530.

行規則（regulation）第 314.4 條[375]第 a 項，美國聯邦貿易委員會（FTC）所監管之金融機構，應指派一名或多名員工，負責協調綜合性資訊安全計畫（information security program），以保護消費者資訊安全性、機密性和完整性。

（三）日本個人資訊保護法

日本現行個人資訊保護法、2020 年 6 月之修正，以及依數位社會整備法提出之修正，皆未包含 DPO 相關規範。但依個人資訊保護委員會指引第 8-3 節舉例說明，指派處理個人資料之負責人並明確責任，係組織性安全管理措施之一[376]。

（四）日本行政機關個人資訊保護法

日本現行行政機關個人資訊保護法，以及依數位社會整備法修正，併入個人資訊保護法之版本，皆未包含 DPO 相關規範。

（五）韓國個人資料保護法

1、指派個資保護官

依韓國個人資料保護法第 31 條第 1 項，個人資料處理者應指派個人資料保護責任者，全權負責個資處理之相關事務[377]。

韓國個人資料保護法施行令第 32 條第 2 項與第 3 項規定了個人資料處理者如何指派個人資料保護責任者。概言之，國家機關、地方政府等的個人資料保護責任者，原則應由達到相應職等的高階公職人員充任。學校及其

[375] 16 CFR 314.4.

[376] 日本，個人情報保護委員会，個人情報の保護に関する法律についてのガイドライン（通則編）（令和 3 年 1 月一部改正），頁 89。

[377] 한국 , 개인정보보호법 , §31(1) , “개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개 인정보 보호책임자를 지정하여야 한다.”

他公務機關之個人資料保護責任者，原則應由行政事務總長、主責個資處理之內部機構長官充任。非公務機關之個人資料保護責任者，應由下列人員充任：(1)業主或代表人；或(2)高階管理人（若無高階管理人，則為主責個資處理之內部機構負責人）。若個人資料處理者係小企業基本法（소상공인기본법）所規定的小企業，則該企業之業主或代表人無需特別指派，自動充任個人資料保護責任者，但該企業另行指派個人資料保護責任者的，不在此限[378]。

2、個資保護官職責及執行職務配套措施

依韓國個人資料保護法第 31 條第 2 項和個人資料保護法施行令第 32 條第 1 項，個人資料保護責任者應履行下列職責：(1)制定並實施個人資料保護計畫；(2)定期檢視並改善個人資料狀態和實際處理狀況；(3)處理個人資料保護相關之申訴與救濟；(4)建置內部控制系統，以防範個人資料之外洩與濫用；(5)制定並實施個人資料保護教育訓練計畫；(6)保護、管理和監督個人資料檔案；(7)擬定、審修和實施個人資料處理政策；(8)管理個人資料保護相關數據；(9)在處理目的達成或儲存期限屆滿後，

[378] 한국，개인정보보호법시행령，§32，“② 개인정보처리자는 법 제 31 조제 1 항에 따라 개인정보 보호책임자를 지정하려는 경우에는 다음 각 호의 구분에 따라 지정한다. 1. 공공기관: 다음 각 목의 구분에 따른 기준에 해당하는 공무원 등…2. 공공기관 외의 개인정보처리자: 다음 각 목의 어느 하나에 해당하는 사람. 가. 사업주 또는 대표자. 나. 임원(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장). ③ 제 2 항에도 불구하고 개인정보처리자가 「소상공인기본법」 제 2 조에 따른 소상공인에 해당하는 경우에는 별도의 지정 없이 그 사업주 또는 대표자를 개인정보 보호책임자로 지정한 것으로 본다. 다만, 개인정보처리자가 별도로 개인정보 보호책임자를 지정한 경우에는 그렇지 않다.

銷毀個人資料[379]。韓國個人資料保護法第 31 條第 2 項並授權以大統領令訂定個人資料保護責任者之其他職責。

依韓國個人資料保護法第 31 條第 3 項，基於履行前開職責所必要，個人資料保護責任者得隨時檢視個人資料處理現況、處理體系等，並得要求相關人員提供報告[380]。依韓國個人資料保護法第 31 條第 5 項，個人資料保護責任者履行前開職務時，個人資料處理者非有正當事由，不得對其施加不利益[381]。

依韓國個人資料保護法第 31 條第 4 項，若個人資料保護責任者知悉任何個人資料保護違法狀況，應立即採取改善措施，並將該等改善措施報告予所屬機構之首長[382]。

由前述規範可知，依韓國個人資料保護法，個人資料處理者有義務指派個人資料保護責任者，全權負責個人資料處理相關事務。個人資料保護責任者原則由個人資料處理者內

379 한국，개인정보보호법，§31(2)，“개인정보 보호책임자는 다음 각 호의 업무를 수행한다. 1. 개인정보 보호 계획의 수립 및 시행. 2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선. 3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제. 4. 개인정보 유출 및 오용・남용 방지를 위한 내부통제시스템의 구축. 5. 개인정보 보호 교육 계획의 수립 및 시행. 6. 개인정보파일의 보호 및 관리・감독. 7. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무.”. 한국，개인정보보호법시행령，§32(1)，“법 제 31 조제 2 항제 7 호에서 “대통령령으로 정한 업무”란 다음 각 호와 같다. 1. 법 제 30 조에 따른 개인정보 처리방침의 수립・변경 및 시행. 2. 개인정보 보호 관련 자료의 관리. 3. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기.”

380 한국，개인정보보호법，§31(3)，“개인정보 보호책임자는 제 2 항 각 호의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.”

381 한국，개인정보보호법，§31(5)，“개인정보처리자는 개인정보 보호책임자가 제 2 항 각 호의 업무를 수행 함에 있어서 정당한 이유 없이 불이익을 주거나 받게 하여서는 아니 된 다.”

382 한국，개인정보보호법，§31(4)，“개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 기관 또는 단체의 장에게 개선조치를 보고하여야 한다.”

部高階人員充任，且並無獨立履行職責要求。個人資料保護責任者原則不得因履行職責而受有不利益。

（六）新加坡個人資料保護法

1、指派個資保護官

依新加坡 PDPA 第 11 條第 3 項規定，組織應指派一名或多名自然人負責PDPA法遵事宜。同條第4項規定，前述指派之法遵負責人，得委託其他自然人履行其職責[383]。新加坡 2021 年個人資料保護細則第 2 條將此兩類自然人合稱為「個資保護官」（以下稱 DPO）。

PDPA 第 11 條第 5 項規定，組織應公開提供至少一名 DPO 之公務聯絡方式，同條第 5A 項舉例說明，若組織依任何法定方式提供 DPO 之公務聯絡方式資訊，則視為已遵守第 5 項之要求[384]。依 PDPA 第 11 條第 6 項，指派 DPO 並不免除組織依 PDPA 負有的任何義務[385]。

2、個資保護官職責及執行職務配套措施

新加坡 PDPA 及 2021 年個人資料保護細則並未詳細列舉 DPO 之職責。由 PDPA 第 11 條第 3 項規定可知，DPO 之核心職責，係確保組織遵守 PDPA。此外，依新加坡 2021 年個人資料保護細則第 3 條，當事人向組織行使個人資料近用權或更正權時，得向 DPO 提出，因此，DPO 之職責，應包括受理當事人近用權和更正權請求。

[383] Singapore, PDPA, §11, "…(3) An organisation shall designate one or more individuals to be responsible for ensuring that the organisation complies with this Act. (4) An individual designated under subsection (3) may delegate to another individual the responsibility conferred by that designation…."

[384] Singapore, PDPA, §11, "…(5) An organisation shall make available to the public the business contact information of at least one of the individuals designated under subsection (3) or delegated under subsection (4). (5A) Without limiting subsection (5), an organisation is deemed to have satisfied that subsection if the organisation makes available the business contact information of any individual mentioned in subsection (3) in any prescribed manner…."

[385] Singapore, PDPA, §11(6), "The designation of an individual by an organisation under subsection (3) shall not relieve the organisation of any of its obligations under this Act."

新加坡個人資料保護委員會於指引中說明[386]，DPO之職責包括但不限於下列各項：(1)確保個資處理政策與程序之制定與實施符合 PDPA；(2)培育組織內部個資保護文化，向利害關係方溝通個資保護政策；(3)管理個資保護相關諮詢與申訴；(4)向管理層提示個人資料相關風險；(5)就個資保護事宜與個人資料保護委員會溝通。

由前述規範可知，依新加坡 PDPA，組織有義務指派個人資料保護官，以確保組織之個資處理行為符合 PDPA。PDPA 並未要求 DPO 獨立履行職責。指派 DPO 並不免除組織依 PDPA 負有的任何義務。

四、法規比較

（一）個資保護官制度之目標

綜觀前述立法例之相關規範，可知目前個資保護官制度尚非各國已普遍採行之制度。比較我國、歐盟、韓國和新加坡關於個資保護官職責及執行職務配套措施之相關規範，可將個資保護官制度大致分為以下幾類：

1、 負責個資安全維護之個資保護官

此類個資保護官之核心職責，係採行安全維護措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。我國個資法之指定專人負責制度即屬此類。

如前所述，我國個資法要求保有個人資料檔案之公務機關指定專人負責個人資料之安全維護事項，而非公務機關依其中央目的事業主管機關訂定之管理辦法，可能須指派專人負責個人資料之安全維護事項。此等專責

[386] Singapore PDPC, Advisory Guidelines on Key Concepts in the PDPA (1 October 2021), paras. 21.4-21.6.

人員可否兼任其他職務、是否需保持獨立性等，並無明確規範。

2、負責執行個資法遵之個資保護官

此類個資保護官之核心職責，係實際執行個資法規之各項要求，確保個人資料蒐集處理利用機關遵守個資法規。韓國個人情報保護法之個人資料保護責任者和新加坡 PDPA 所規定之 DPO 皆屬此類。

韓國個人資料保護責任者實際負責個資保護制度建置、當事人申訴處理、個資安全維護等。個人資料保護責任者依法由個人資料處理者之業主或內部高階人員充任，並不要求獨立性。新加坡 DPO 可由組織內部或外部人員擔任，比韓國更強調 DPO 之資料保護專業知識，且強調 DPO 係輔助性職責，組織並不因指派 DPO 而免負法遵責任，亦未要求 DPO 獨立履行職責。

3、負責監督個資法遵之個資保護官

此類個資保護官之核心職責，係協助個人資料蒐集處理利用機關遵守個資法規，並承擔諮詢與監督職能。歐盟 GDPR 所規定之 DPO 制度即屬此類。歐盟 GDPR 強調 DPO 之諮詢與監督職能，要求 DPO 獨立履行職責，嚴格避免利益衝突，且不得因履行職責而受不利對待。

（二）指派個資保護官之義務

我國及其他各國強制指派個資保護官之要求，與個資保護官之職責相適應。

我國個資法要求指派專人負責安全維護事項。因此，須注重個人資料安全之機關，例如公務機關，以及目的事業主管機關指定之非公務機關，強制指派專人負責。

韓國個人資料保護法要求個人資料處理者指派個人資料保護責任者，「全權負責」個資處理之相關事務。因此，所有個人資料處理者皆須指派個人資料保護責任者，且非公務機關之個人資料保護責任者通常由業主擔任。從本質上考量，依我國個資法指定之「專人」，與依韓國個人資料保護法指派之「個人資料保護責任者」之角色是一致的，惟負責範圍有差別，我國個資法指定之「專人」，其職責係韓國個人資料保護責任者職責之一部分。

新加坡 PDPA 所規定之 DPO 實際執行組織之個資法遵事務，故各組織皆應指派一名或多名。PDPA 強調 DPO 係一輔助性專業職務，因此在委託他人履行職責、兼任等方面要求較寬鬆。

歐盟 GDPR 所規定之 DPO 係監督控管者或處理者之個資法遵狀況，且對 DPO 之獨立性有嚴格要求。因此在公務機關，或控管者或處理者之核心業務所涉個資處理作業，需大規模經常性且系統性監控當事人、大規模處理特種個資或前科或犯罪個資之高風險情形，強制指派 DPO。

各國個資法規關於本議題之比較表格整理如下：

表 7、各國個資保護官相關規範比較表

國家	權利內容	法源依據	位階
臺灣	資料蒐集、處理或利用機關之安全維護措施，得包括「配置管理之人員及相當資源」。	個人資料保護法施行細則第 12 條第 2 項第 1 款	主管機關命令
歐盟	下列情形下，應指派 DPO： (1) 公務機關處理個人資料； (2) 控管者或處理者之核心活動	GDPR§37-39	法律

國家		權利內容	法源依據	位階
		需經常、系統性且大規模地監控個資當事人； (3) 控管者或處理者之核心活動需大規模處理敏感個資或前科、犯罪相關個資。		
美國	聯邦	適用 HIPAA 之受管轄機構（covered entity）須指派隱私官（privacy official），負責建置與實施該機構的政策與程序。	HIPAA Regulation §164.530(a)(1) (45 CFR § 164.530(a)(1))	
		美國聯邦貿易委員會（FTC）所監管之金融機構，應指派一名或多名員工，負責協調綜合性資訊安全計畫（information security program），以保護消費者資訊安全性、機密性和完整性。	GLBA Regulation §314.4(a) (16 CFR § 314.4(a))	
	加州	加州個資法規並未規定業者須設置 DPO 之規範。	-	-
	維吉尼亞州	維吉尼亞州個資法規並未規定業者須設置 DPO 之規範。	-	-

國家	權利內容	法源依據	位階
日本	指派個人資料保護責任者，為組織性安全管理措施之一。	個人資料保護委員會指引第 8-3 節	主管機關指引
韓國	個人資料處理者應指派「個人資料保護責任者」，全權負責個人資料處理之相關業務，例如： (1)制定並實施個人資料保護計畫； (2)處理個人資料相關之投訴處理及被侵害救濟。	個人資料保護法 §31	法律
新加坡	組織應指派至少一名人員負責 PDPA 法遵事宜，並公開相關聯絡方式。	PDPA §11	法律

五、修法需求分析與本節結論

綜合本節比較研究，本報告發現，目前個資保護官制度尚非各國已普遍採行之制度。我國個資法要求公務機關指定專人負責個人資料安全維護事項，但其履行職責之方法及配套措施，並不明確。而觀察國外立法例可知，歐盟、韓國和新加坡之個資保護官制度雖職責定位不同，但皆是負責個資法遵之整體流程，而非聚焦於個人資料之安全維護事項。

依前文法規比較所示，國外個資保護官之角色定位，包括「執行個資法遵」與「監督個資法遵」兩類，其職責內容、獨立性、執

行職務保障等方面之要求不儘相同。前者實際參與個資法各項制度之建置與執行，後者則居於諮詢監督角色，獨立性較高。

考量個人資料蒐集處理利用機關依個資法所負義務，不限於個人資料之安全維護，尚包括確保資料之蒐集處理利用符合個資法規範、答覆當事人權利行使請求、與主管機關溝通等，我國似可考慮調整現行指定專人負責「個資安全維護事項」之制度，將其擴充為由專人負責「個資法令遵循」事項。又我國 107 年頒行之資通安全管理法要求公務機關應置「資通安全長」，負責推動及監督機關內資通安全相關事務。因資通安全與個人資料保護間關聯密切，公務機關不乏將個資法所要求指定之「專人」與「資通安全長」結合者。例如，衛生福利部設置「資通安全治理暨個人資料保護會」，通掌個資安全維護與資安事項。我國個資法未來如調整第 18 條規範，似可考慮與現行資通安全長制度之調和與銜接。

然而，全面負責「個資法遵」之個資保護官對於我國而言，可謂一項全新制度，將在相當程度上對社會及行業造成衝擊。是宜由主管機關在擬訂個資法修正草案時，先行評估我國個資法律制度之法遵協助需求，確定 DPO 之角色，係實際執行法遵事項，抑或是提供個資法遵之監督與諮詢，以決定個資法對此議題的調整方向。

第四章　研究結論

綜合前文對研究議題之比較分析可知，本研究所涉議題於我國現行個資法似均有調整、補充之空間，梳理如下：

一、當事人拒絕權

個資法宜就下列蒐集、處理與利用個人資料之合法要件，以及蒐集機關利用個人資料的自動化決策行為，藉由原則與例外的法益價值安排，適當賦予當事人對蒐集機關表示拒絕之權，並調整舉證責任。

（一）在適用「當事人自行公開或已合法公開」的情形，蒐集機關倘無從適用其他合法要件，宜適當賦予當事人拒絕之權。

（二）在適用「研究條款」的情形，如資料提供者未先將資料去識別後提供，應許當事人拒絕，並由蒐集或提供個人資料之機關承擔優勢公益及不將資料去識別之必要性的舉證之責，較能兼顧當事人的權利保障。

（三）在適用「公益條款」的情形，考量其為不確定法律概念且有高低程度不同之別，個資法宜適當賦予當事人拒絕權，由蒐集機關承擔優勢公益的舉證責任，應較能緩和由蒐集機關單方主張公益條款即蒐集、處理與利用當事人個人資料所造成的衝突。

（四）在主張「對當事人權益無侵害」的情形，本款單以該行為對當事人權益有無侵害作為考量，未將該行為是否對蒐集機關具有正當利益納入要素，則似宜賦予當事人適當之拒絕權，降低當事人若認為該行為侵害其權益，尚須向蒐集機關爭執之成本。

（五）在主張「有利於當事人權益」的情形，由於本款規定單以該行為是否有利於當事人權益為斷，並不考量蒐集機關對該利用行為是否具有正當利益，則倘當事人不願享受該權益，應無不許之理，個資法宜對本款事由適當賦予當事人拒絕權。

（六）參酌歐盟 GDPR 之精神，適當增加當事人對於自動化決策行為拒絕權之原則與例外。

據此，本研究建議於個資法第 11 條，增訂當事人於上述情形下，請求公務機關或非公務機關停止蒐集、處理或利用其個人資料之原則與例外規範，修正條文草案詳見後文第五章。

又我國個資法對非公務機關利用個人資料行銷之行為，賦予當事人無條件的拒絕之權，並要求非公務機關於首次行銷時，向當事人提供免付費拒絕行銷之方式。本研究建議就非公務機關如何踐行個資法前揭要求、落實當事人之行銷拒絕權訂定指引（草案詳附件 1），俾利非公務機關依循。

二、當事人查閱或請求閱覽權

為明確數位足跡屬於個人資料，提示業者和網路使用者依個資法蒐集處理利用數位足跡，強化當事人就數位足跡行使資料權利之保障，我國似可考慮在關於「個人資料」之條文，增列數位足跡之相關例示。考量我國個資保護法制體系架構，本研究認為數位足跡之例示增列於個資法施行細則中，條文草案詳見後文第五章。

又考量數位足跡在內容、蒐集、儲存、管理等諸多方面之特殊性，本研究建議就當事人如何行使個資法上查閱權制定指引，以協助公務機關或非公務機關回應當事人查閱請求，詳參附件 2。

三、告知目的外利用或自動化決策之告知義務

個資法宜適當導入目的外利用個人資料的告知義務之原則與例外規範，一方面賦予當事人知情機會，另方面平衡考量當事人的權利受限程度與蒐集者目的外利用個人資料所追求之目的，建構權利保障與合理利用個人資料之框架。此修法方向可由兩方面著手，其一為參考個資法第 8 條與第 9 條對於蒐集時告知義務的例外規定，移植適當例外條款適用於目的外利用個人資料情形；其二則係依個資法第 16 條與第 20 條所列得目的外利用個人資料之事由，逐一檢視應

否就個別情形課予蒐集者於目的外利用個人資料時的告知義務。對此，本研究建議於個資法增訂第九條之一，明定公務機關或非公務機關個資目的外利用前向當事人踐行告知之義務，並於個資法施行細則第十六條補充目的外利用告知方式之規範，條文草案詳如後文第五章。

至於自動化決策之告知與否，由於此行為可視為利用個人資料之方式之一，應屬於個資法第 8 條第 1 項第 4 款的告知義務範圍，歐盟 GDPR 獨立對此訂定規範，毋寧認為係因 GDPR 賦予當事人對自動化決策的拒絕權，是特別要求控管者應向當事人揭露自動化決策之事實與當事人可拒絕之權利。因此此處應與拒絕權之增訂一併評估，如於我國個資法新增當事人對於自動化決策之拒絕權，即應一同強調蒐集機關對當事人揭露自動化決策之事實的義務。因此，本研究認為，我國可於個資法施行細則中，明確以個資作自動化決策者，應踐行告知義務，條文草案詳如後文第五章。

四、個資外洩通知

個資法在個資侵害事故通知當事人方面，係以侵害事故發生機關之違法性作為判斷標準，未呈現對當事人權益風險之考量。而在通報主管機關方面，我國個資法並無個資侵害事故通報主管機關之明文規範，現行通報制度係由非公務機關之中央目的事業主管機關分別訂定，尚欠缺統一性通報標準。

為進一步落實現行個資法保障個資當事人權益之立法目的，可思考調整現行通知當事人之判定標準，引入當事人權益風險之考量要素，同時於個資法中，規範個資侵害事故通報標準，並參照資通安全管理法相應規範，構建個資侵害事故通報制度。

因此，本研究建議修正現行個資法第 12 條關於通知當事人之規定，並建議增訂第 12 條之 1 關於通報主管機關之規定，條文草案詳如後文第五章。

惟於尚未修正個資法調整現行個資侵害事故通知當事人之判定標準的情況，本研究建議修正個資法施行細則第 22 條，以其他用語取代「需費過鉅」，條文修正草案詳如後文第五章；並搭配該條之修正，提供通知當事人之內容及方式指引草案，如附件 3。

五、當事人同意

考量當事人同意乃我國個資法規範蒐集、處理與利用個人資料之合法要件之一，違反者將面臨刑事、行政或民事責任，若僅以主管機關發布指引或函釋之方式闡明同意「自主性」、「特定性」、「知情性」、「明確性」與「可撤回性」要件，恐於「法律明確性」之檢視產生爭議。本報告據此認為，我國宜於個資保護法令規範中以適當文字納入前述同意之要件。考量我國個資保護法制體系架構，本研究建議於施行細則中增訂前開同意條件，架構有效的當事人同意法規框架，相關條文草案於後文第五章敘明。

六、個資衝擊影響評估

從強化當事人資訊隱私權保障之角度，我國似可考慮調整並擴充個資衝擊影響評估制度，由對資料安全風險之評估轉型為對當事人權益風險之評估。惟此一轉變必然將增加公務及非公務機關個資保護法令遵循之難度與成本。為減緩對我國社會及行業之衝擊，並考量個人資料蒐集處理利用所涉之風險，我國個資法似可考慮將強制性當事人權益風險評估之適用範圍限定於公務機關及特定個資保護風險較高之非公務機關。

惟如主管機關在擬訂個資法修正草案過程中，經評估認為當事人權益風險評估模式對於我國社會與行業之衝擊仍嫌過重，亦可思考維持現行資料安全評估模式，並參酌韓國個人資料保護法相關內容，在我國個資法施行細則中，增訂定安全風險類別、適用範圍、評估標準、安全考量事項、具體步驟、評估結果處理方式等細部規範。

就前揭兩種修法策略，本研究建議分別提出個資法、個資法施行細則之相關條文修正草案（詳第五章），並配合細則之修訂，提供指引草案如附件 4。

七、個資保護官

考量個人資料蒐集處理利用機關依個資法所負義務，不限於個人資料之安全維護，尚包括確保資料之蒐集處理利用符合個資法規範、答覆當事人權利行使請求、與主管機關溝通等，我國似可考慮調整現行指定專人負責「個資安全維護事項」之制度，將其擴充為由專人負責「個資法令遵循」事項。

然而，全面負責「個資法遵」之個資保護官對於我國而言，可謂一項全新制度，將在相當程度上對社會及行業造成衝擊。是宜由主管機關在擬訂個資法修正草案時，先行評估我國個資法律制度之法遵協助需求，確定個資保護官之角色，係實際執行法遵事項，抑或是提供個資法遵之監督與諮詢，以決定個資法對此議題的調整方向。

第五章　修法條文與指引草案

承接前文研究結論，研究團隊就本研究所涉議題，提出下列個資法（包含施行細則）的建議修正條文草案對照表，作為我國個資法調適的參考依據。本研究並就特定議題提供指引草案，以提示相關優良實務作法，作為公務機關或非公務機關遵循個資法相關規範之參考。指引草案皆定位為不具法令拘束力之參考文件，不影響司法機關或各目的事業主管機關本於權責對個資法及施行細則之解釋與適用[387]，先予敘明。

一、當事人拒絕權

（一）修正個資法條文，增訂當事人對合法蒐集、處理、利用個資之行為行使拒絕權之原則與例外。修正條文草案如下：

表 8、拒絕權相關條文修正草案對照表

修正條文	現行條文	說明
第十一條 I 公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。 II 個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行職務或業	**第十一條** I 公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。 II 個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行職務或業	一、為強化當事人權利保障，新增第十一條第五項，使當事人對蒐集機關特定合法蒐集、處理或利用個人資料之行為，亦有權拒絕。 二、當事人自行公開個人資料之目的不一，法律規定應公開之個人

[387]有關法規主管機關就其主管法規，對不相隸屬之其他機關所為之一般、抽象性之解釋(例如函釋、指引等)，性質非屬行政規則，現行行政程序法對其法律效果尚無明文規定，惟參考行政程序法修正草案第 162 條之 2，對此增訂相關規定，並明定其性質準用行政規則，以資明確。行政程序法修正草案第 162 條之 2：「法規主管機關就其主管法規，對不相隸屬之其他機關所為具有一般抽象法律見解之解釋，應公開於機關網站所設置之法規查詢專區，並準用第一百六十條第三項及第一百六十二條第一項之規定」。

務所必須，或經當事人書面同意，並經註明其爭議者，不在此限。 III 個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。 IV 違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。 V 有下列情形之一者，公務機關或非公務機關雖未違反本法規定蒐集、處理或利用個人資料，仍應依當事人之請求，停止蒐集、處理或利用其個人資料： 一、依第六條第一項但書第三款或第十九條第一項第三款規定，蒐集、處理或利用個人資料。	務所必須，或經當事人書面同意，並經註明其爭議者，不在此限。 III 個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。 IV 違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。 V 因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。	資料亦有該法追求之正當目的。雖在當事人自行公開或經合法公開個人資料之情形，對當事人隱私侵害程度較小，但仍應適度保障當事人對其個人資料之自主權，爰增訂第十一條第五項第一款之拒絕事由。 三、現行法允許公務機關或學術研究機構於符合特定之目的時，為統計或學術研究而有必要者，提供尚未達到無從識別特定之當事人程度之個人資料予第三人（蒐集者），將使蒐集者在保有該個人資料之期間，仍有識別特定當事人之可能，爰增訂第十一條第五項第二款之拒絕事由，平衡保障當事人之權利。

二、依第六條第一項但書第四款、第十六條但書第五款、第十九條第一項第四款或第二十條第一項但書第五款規定，蒐集、處理或利用個人資料，且蒐集者以其所保有之資訊，得以識別特定之當事人。 三、依第十六條但書第二款後段、第十九條第一項第六款或第二十條第一項但書第二款規定，蒐集、處理或利用個人資料。但能證明所追求之公共利益顯優於當事人之權益者，不在此限。 四、依第十五條第三款或第十九條第一項第八款規定，蒐集、處理個人資料。 五、依第十六條但書第六款或第二十條第一項但書第七款規定，利用個人資料。 VI公務機關或非公務機關僅以自動化決策對當事		四、考量公共利益為不確定法律概念，並應有高低程度之別，爰增訂第十一條第五項第三款之拒絕事由，使當事人得對機關以增進公共利益所必要為蒐集、處理或利用個人資料之依據時，得對該機關行使拒絕權。惟該機關能證明所追求之公共利益明顯優於當事人之權益者，不在此限（例如非公務機關於寄送當事人的帳單內或信封上配合政府機關刊載政令宣導時，如所涉之政令宣導為「防疫三級警戒期間注意事項」，依當前時空與社會背景，應可認所追求的公共利益顯優於當事人權益；如所涉為「社會住宅包租代管試辦計畫」，因該政策較無急迫性、

人作成具有法律效果或類似重大效果之決定者，當事人有權拒絕而不受該決定之拘束。但有下列情形之一，且蒐集機關已提供當事人請求人為介入自動化決策，並對自動化決策陳述意見之機會者，不在此限： 一、自動化決策為締結或履行蒐集機關與當事人間之契約或類似契約所必要。 二、經當事人同意。 VII 因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。		適用範圍相對較窄，且政府機關應可以其他方式實現宣傳目的，似可認所追求的公共利益非顯優於當事人權益）。 五、現行法允許機關於對當事人權益無侵害之情形，蒐集、處理當事人之個人資料。由於該情形僅以行為對當事人權益有無侵害為考量，爰增訂第十一條第五項第四款之拒絕事由，以尊重當事人對權益遭受侵害與否之判斷。 六、現行法允許機關在有利於當事人權益之情形，於目的外利用個人資料。由於該情形僅以行為是否有利於當事人權益為考量，爰增訂第十一條第五項第五款之拒絕事由，以尊重當事人對

		該行為有利於其權益與否之判斷。 七、考量數位時代下的資料蒐集、探勘與分析技術日新月異，各種人工智慧、演算法與大數據的搭配應用層出不窮，自動化決策將是機關創造資料價值的重要工具。倘當事人對機關的自動化決策全無置喙餘地，恐難以避免類似資訊歧視、區別待遇等對當事人不公平之情事發生。爰參考歐盟GDPR第22條規定，增訂第十一條第六項，使當事人有權拒絕機關僅以自動化決策對當事人作成具有法律效果或類似重大效果之決定。 八、原第十一條第五項移列至同條第七項。
第二條	**第二條**	配合本法新增第十一條第六項關於自動化決策拒絕

本法用詞，定義如下： 一、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。 二、個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。 三、蒐集：指以任何方式取得個人資料。 四、處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。	本法用詞，定義如下： 一、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。 二、個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。 三、蒐集：指以任何方式取得個人資料。 四、處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。	權之規定，增訂第二條第十款與第十一款名詞定義。

五、利用：指將蒐集之個人資料為處理以外之使用。 六、國際傳輸：指將個人資料作跨國（境）之處理或利用。 七、公務機關：指依法行使公權力之中央或地方機關或行政法人。 八、非公務機關：指前款以外之自然人、法人或其他團體。 九、當事人：指個人資料之本人。 十、自動化決策：指以各種技術方式，無人為參與而利用個人資料對當事人作出決策，包含利用已蒐集之個人資料、觀察個人行為所得之資料、衍生或推論之個人資料、剖析之個人資料、結合其他個人資料或非個人資料所為之決定。 十一、 剖析：指評估、分析或預測當事人之能力、經濟、健康、	五、利用：指將蒐集之個人資料為處理以外之使用。 六、國際傳輸：指將個人資料作跨國（境）之處理或利用。 七、公務機關：指依法行使公權力之中央或地方機關或行政法人。 八、非公務機關：指前款以外之自然人、法人或其他團體。 九、當事人：指個人資料之本人。	

偏好、興趣、信用、行為、位置、行蹤或其他與當事人有關之條件或狀態。		

（二）針對拒絕行銷訂定指引草案（附件 1）

二、當事人查閱權

（一）修正個資法施行細則，增訂數位足跡為個人資料之例示。修正條文草案如下：

表 9、查閱權相關條文修正草案對照表

修正條文	現行條文	說明
第四條 I 本法第二條第一款所稱病歷之個人資料，指醫療法第六十七條第二項所列之各款資料。 II 本法第二條第一款所稱醫療之個人資料，指病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方、用藥、施術或處置所產生	**第四條** I 本法第二條第一款所稱病歷之個人資料，指醫療法第六十七條第二項所列之各款資料。 II 本法第二條第一款所稱醫療之個人資料，指病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方、用藥、施術或處置所產生	使用者於網路活動所產生或與之相關之資料，如網路識別碼、網路活動紀錄，以及網路產品或服務提供者據此推知之使用者相關資訊等，如得以直接或間接方式識別特定個人，自屬我國個人資料保護法（以下稱個資法）所稱之個人資料，而有個資法關於蒐集機關義務、當事人權利等規範之適用。參酌歐盟 GDPR、美國加州《消費者隱私法》（CCPA）皆明文將該等資料列為個人資料之例

之個人資料。 III 本法第二條第一款所稱基因之個人資料，指由人體一段去氧核醣核酸構成，為人體控制特定功能之遺傳單位訊息。 IV 本法第二條第一款所稱性生活之個人資料，指性取向或性慣行之個人資料。 V 本法第二條第一款所稱健康檢查之個人資料，指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料。 VI 本法第二條第一款所稱犯罪前科之個人資料，指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄。 VII 本法第二條第一款所稱個人資料，包括因使用網路產品或服務所產生，或與該使用相關，且得以直接或間接識別該個人之資料，如網路識別碼、網路活動紀錄及基於	之個人資料。 III 本法第二條第一款所稱基因之個人資料，指由人體一段去氧核醣核酸構成，為人體控制特定功能之遺傳單位訊息。 IV 本法第二條第一款所稱性生活之個人資料，指性取向或性慣行之個人資料。 V 本法第二條第一款所稱健康檢查之個人資料，指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料。 VI 本法第二條第一款所稱犯罪前科之個人資料，指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄。	示，爰增訂第七項，以利樹立公務機關、非公務機關及當事人之正確認知，強化當事人個人資料自主權保護。

網路活動而推知之資料。		

（二）就數位足跡如何行使查閱權及其範圍訂定指引草案（附件 2）

三、告知目的外利用或利用開放資料為自動化決策之告知

（一）參考個資法第 8 條與第 9 條的蒐集告知例外條款之立法方式，修正個資法，納入目的外利用的告知原則與例外。修正條文草案對照表如下：

表 10、目的外利用告知相關條文草案對照表

修正條文	現行條文	說明
第七條 I 第十五條第二款及第十九條第一項第五款所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。 II 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第九條之一第一項各款應告知事項及同意與否對其權益之影響後，單獨所為之意思表示。 III 公務機關或非公務機關明確告知當事人第八條	**第七條** I 第十五條第二款及第十九條第一項第五款所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。 II 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。 III 公務機關或非公務機關明確告知當事人第八條	配合第九條之一關於目的外利用告知之規定，爰將本條第二項「特定目的外之其他利用目的、範圍」修正為「第九條之一第一項各款應告知事項」。

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。 IV 蒐集者就本法所稱經當事人同意之事實，應負舉證責任。	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。 IV 蒐集者就本法所稱經當事人同意之事實，應負舉證責任。	
第九條之一 I 公務機關或非公務機關依第十六條但書或第二十條第一項但書規定利用個人資料時，應於利用前明確向當事人告知下列事項： 一、 公務機關或非公務機關名稱。 二、 利用之目的。 三、 利用之個人資料或其類別。 四、 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。 II 有下列情形之一者，得		一、 為保障當事人充分瞭解資料蒐集之目的及用途，第八條第一項和第九條第一項已明定蒐集前向當事人告知法定事項之義務。惟蒐集機關於目的外利用個人資料時，亦應保障當事人對該利用行為之充分瞭解，爰參酌歐盟GDPR、美國加州《消費者隱私法》（CCPA）等規定，增訂本條，明文要求蒐集機關目的外利用個人資料前，向當事人告知法定

免為前項之告知： 一、依法律規定得免告知。 二、個人資料之利用係公務機關執行法定職務或非公務機關履行法定義務所必要。 三、告知將使公務機關或非公務機關違反法律規定之保密義務。 四、當事人明知應告知之內容。 五、不能或需勞費過鉅始能向當事人或其法定代理人為告知。 六、告知將損害當事人或他人之生命、身體或財產利益，或有損害之虞。 七、告知將嚴重損害利用機關之權利或正當利益。 III 前項第五款情形，利用機關應將第一項各款事項以適當方式公告。		事項，以利增強個資目的外利用之透明性，強化當事人個人資料自主權。 二、於個資當事人聯絡方式不明、涉及大量個資當事人等情形，可能客觀上無法直接向當事人逐一告知本條所列事項，或告知將需過鉅勞費。爰於第二項第五款及第三項規定，得以公告方式為之。
個資法施行細則		

第十六條 I 依本法第八條、第九條、第九條之一第一項及第五十四條所定告知之方式，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。 II 本法第九條之一第三項所稱適當方式公告，指斟酌技術之可行性及當事人隱私與其他權利之保護，以網際網路、新聞媒體或其他適當公開方式為之。	**第十六條** 依本法第八條、第九條及第五十四條所定告知之方式，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。	一、 配合個資法增訂第九條之一，爰修正第一項。 二、 個資法第九條之一允許目的外利用告知需費過鉅時，以公告方式為之，爰增訂第二項，明確公告之執行方式與考量要素。

（二）修正個資法施行細則，闡明個資法第 8 條之告知義務包括自動化決策之利用目的或方式。修正條文草案對照表如下：

表 11、自動化決策告知相關修正條文草案對照表

修正條文	現行條文	說明

第十六條之一 一、公務機關或非公務機關以個人資料為自動化決策者，應依本法關於告知當事人之規定，向當事人告知該自動化決策之目的與利用方式。 二、前項情形，如公務機關或非公務機關將依自動化決策對當事人作成具有法律效果或類似重大效果之決定者，所告知之個資蒐集目的與利用方式，應包含該自動化決策所涉邏輯、對當事人之影響及預期後果，且該告知應以簡明易懂之方式為之。	（本條新增）	一、將個人資料用於自動化決策，係個人資料之利用行為之一，自應依本法相關規定，向當事人告知其目的與方式，爰增訂第一項，以資明確。 二、若自動化決策所作決定將對當事人有法律效果或類似重大效果，則應保障當事人知悉該等決策之運作原理與影響之權利。爰參酌歐盟 GDPR 第 13 條、第 14 條之規範，增訂第二項。

四、個資外洩通知

（一）修正個資法，增訂將個資侵害事故通報主管機關之要求，並調整現行個資侵害事故通知當事人之判定標準，引入當事人權益風險之考量要素。修正條文草案對照表如下：

表 12、個資侵害事故通知當事人修法條文草案對照表

修正條文	現行條文	說明
第十二條 公務機關或非公務機關發生個人資料被竊取、洩漏、竄改或其他侵害，可能導致當事人隱私或其他權利受侵害之高度風險者，應以適當方式通知當事人，不得無故遲延。	**第十二條** 公務機關或非公務機關違反本法規定，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。	一、個人資料侵害事故與違反本法規定間之因果關係往往難以判斷，且查明可能需相當時間，為防止通知當事人不當遲延，爰將「違反本法規定」與「查明後」予以刪除，並規定「不得無故遲延」，以保障當事人及時獲得通知。 二、鑒於個人資料侵害事故程度不一，為保護當事人免受通知疲勞，並適當衡平事故發生機關之通知成本，參酌歐盟GDPR、日本《個人資訊保護法》、新加坡《個人資料保護法》（PDPA）等關於個人資料侵害事故通知當事人之規範，爰增訂侵

		害可能導致當事人權利保護高風險者，方需通知當事人。
第十二條之一 （甲案） 中央目的事業主管機關業依第二十七條第二項及第三項授權訂定辦法者，適用該辦法之非公務機關發生個人資料被竊取、洩漏、竄改或其他侵害者，應於知悉該侵害事故後七十二小時內通報中央目的事業主管機關或直轄市、縣（市）政府 （乙案） 非公務機關發生個人資料被竊取、洩漏、竄改或其他侵害者，應於知悉該侵害事故後七十二小時內通報中央目的事業主管機關或直轄市、縣（市）政府。但中央目的事業主管機關依第二十七條第二項、第三項授權訂定之辦法就通報對象、方式等事	（本條新增）	（甲案） 為確保個人資料侵害事故發生時，主管機關對事故發生機關因應狀況之有效監督、及時給予行政指導，參酌歐盟 GDPR、日本《個人資訊保護法》、新加坡《個人資料保護法》（PDPA）等關於個資侵害事故通報主管機關之要求，爰增訂本條，並考量於中央目的事業主管機關已訂有安維辦法之非公務機關，原則上無管轄權爭議之疑慮，於發生個資侵害事故時，應於時限內通報其中央目的事業主管機關。 （註：甲案優點在於通報對象特定，且無管轄權爭議，較無執行阻礙；缺點在於中央目的事業主管機關未訂定安維辦法之非公務機關，則恐生無須通報之爭議。）

項另有規定者，從其規定。 前項通報對象有疑義者，非公務機關得通報各有權管轄之中央目的事業主管機關與直轄市、縣（市）政府。		（乙案） 一、為確保個人資料侵害事故發生時，主管機關對事故發生機關因應狀況之有效監督、及時給予行政指導，參酌歐盟 GDPR、日本《個人資訊保護法》、新加坡《個人資料保護法》（PDPA）等關於個資侵害事故通報主管機關之要求，爰增訂本條第一項本文，明定非公務機關於個資侵害事故發生時，應通報中央目的事業主管機關或直轄市、縣（市）政府。 二、又如中央目的事業主管機關依本法授權，於法規命令中就個資侵害事故通報之對象或方式已有規定者，非公務機關即應從其規定，爰增訂第一項但書規定。 三、另若非公務機關對應

		通報之對象尚有疑義時，為使主管機關及時掌握個資侵害事故，非公務機關仍應先行通報有權管轄之主管機關，爰增訂第二項。如受通報之主管機關就管轄有爭議者，應由本法主管機關統一解釋。 （註：此案優點在於無論中央目的事業主管機關是否已依本法授權訂定法規命令，非公務機關於發生個資侵害事故時，均應通報；缺點在於當管轄不明或有爭議時，不同主管機關受理通報後倘仍需費時釐清管轄，恐延遲事故調查時程。）
第四十八條 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰：	**第四十八條** 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰：	配合增訂第十二條之一個資侵害事故通報主管機關之規範，調整罰則。

一、違反第八條或第九條規定。 二、違反第十條、第十一條、第十二條、第十二條之一或第十三條規定。 三、違反第二十條第二項或第三項規定。 違反第二十七條第一項或未依第二項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。	一、違反第八條或第九條規定。 二、違反第十條、第十一條、第十二條或第十三條規定。 三、違反第二十條第二項或第三項規定。 違反第二十七條第一項或未依第二項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。	

（二）於尚未修正個資法調整現行個資侵害事故通知當事人之判定標準的情況，建議修正個資法施行細則第 22 條，以其他用語取代「需費過鉅」。修正條文草案對照表如下：

表 13、個資侵害事故通知當事人施行細則修正條文草案對照表

修正條文	現行條文	說明
第二十二條 I 本法第十二條所稱適當方式通知當事人，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但	**第二十二條** I 本法第十二條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過	一、 參酌歐盟 GDPR、日本《個人資訊保護法》、新加坡《個人資料保護法》（PDPA）等關於個人資料侵害事故通知當事人之規範，皆根據侵害事故所

侵害所致當事人隱私及其他權利保護風險較低或通知所需勞費過鉅者，得斟酌技術之可行性及當事人隱私與其他權利之保護，以網際網路、新聞媒體或其他適當公開方式為之。 II 依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。	鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。 II 依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。	致當事人權益風險，區分不同處理方式，以保護當事人免受通知疲勞，並適當衡平事故發生機關之通知成本。爰修正本條第一項，明定當事人之個人資料遭受外洩等侵害事故，如通知所需勞費過鉅或所致隱私及其他權利風險較低，則允許公務機關或非公務機關以網際網路等公開方式為通知。 二、 公務機關或非公務機關通知當事人之成本，除所需經費外，尚包括所耗人力、時間等，故將「需費過鉅」酌修正為「勞費過鉅」。 三、 公開通知方式如選擇不當，對當事人權利之影響未必以隱私為限，故增訂

		其他權利亦為確定適當公開通知方式之考量事項。

（三）於尚未修正個資法調整現行個資侵害事故通知當事人之判定標準的情況，搭配前述個資法施行細則第 22 條之修正，就通知當事人之內容及方式訂定指引草案（附件 3）

五、當事人同意

修正個資法施行細則，補充同意之要件。修正條文草案對照表如下：

表 14、當事人同意相關修正條文草案對照表

修正條文	現行條文	說明
第十四條之一 I 本法所稱同意，指當事人對個別特定目的，基於自由意願將其允許之意思，以積極行為所為之表示。 II 當事人未同意或事後撤回同意，均不致使既有權益遭受不利。 III 第一項所稱積極行為，指當事人清楚肯定表達其同意意思之行動。	（本條新增）	一、當事人同意乃蒐集、處理或利用個人資料的合法事由之一，同意應具自主性、特定性、明確性等特徵，方符保障當事人資料自主權之意旨，爰增訂本條，以利明確有效同意之要件。 二、同意應於可行範圍內，針對個別特定目的分別為之，以保障當事人決定其個人資料是否用於

		特定目的之自主權，爰於第一項規定同意係當事人「對個別特定目的」為之。 三、 同意應由當事人基於自由意願給予，未同意或事後撤回同意，不得影響其同意前之原有權益（例如「不因不同意而須支付較高費用」、「不因不同意而減損服務效能」，以及「不因不同意目的外利用而影響原有目的下的權利」等情形），爰增訂第二項。 四、 參酌歐盟GDPR、韓國《個人資料保護法》、美國《加州消費者隱私法（CCPA）》等規範。

六、個資保護影響評估

（一）修正個資法，增訂強制執行個資保護影響評估之情形。修正條文草案對照表如下：

表 15、個資保護影響評估修法條文草案對照表

修正條文	現行條文	說明
第十八條 I 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。 II 公務機關蒐集、處理或利用個人資料之行為，或該行為涉及之系統，依其性質、背景、目的與範圍，對當事人權益有高風險之虞者，應於行為前或系統使用前，執行個人資料保護影響評估。 III 有下列情形之一者，視為前項所稱對當事人權益有高風險之虞： 一、 對當事人為評估或預測（包含剖析）。 二、 具有法律效果或類似	**第十八條** I 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。	為強化公務機關之問責性，課予公務機關事先識別其行為對個人資料當事人權益造成潛在風險之責任，俾使公務機關得事先採取各項風險因應措施，爰參考歐盟 GDPR 第 35 條規定，增訂第十八條第二項至第五項關於個人資料保護影響評估之規範，落實公務機關之資料治理責任。

重大效果之自動化決策。 三、對當事人之系統性監控。 四、涉及本法第六條之個人資料。 五、依涉及人數、資料數量、持續時間等條件，大規模蒐集、處理或利用個人資料。 六、匹配或組合不同資料集。 七、蒐集、處理或利用弱勢當事人之個人資料。 八、創新利用或應用新的技術性或組織性解決方案。 九、該行為將阻止當事人行使權利、使用服務或締結契約。 IV 第二項所稱個人資料保護影響評估，至少應包括下列事項： 一、識別蒐集、處理或利用個人資料之行為、範圍與流程。 二、檢視蒐集、處理或		

利用個人資料之合目的性與合比例性。 三、評估個人資料蒐集、處理或利用行為對當事人隱私及其他權益之風險。 四、規劃風險因應措施。 V 公務機關應依個人資料保護影響評估結果，採取規劃之風險因應措施以避免或降低風險，並應持續監控剩餘風險，即時改善風險因應措施之有效性。		
第二十七條之一 非公務機關蒐集、處理或利用個人資料之行為，或該行為涉及之系統，依其性質、背景、目的與範圍，對當事人權益有高風險之虞者，應於行為前或系統使用前，執行個人資料保護影響評估。評估之執行條件、內容與方式，準用第十八條第三項至第五項規定。	（本條新增）	為強化非公務機關之問責性，爰參考歐盟 GDPR 第 35 條規定，增訂第二十七條之一關於個人資料保護影響評估規範，並準用第十八條第三項至第五項。

第四十八條 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰： 一、違反第八條或第九條規定。 二、違反第十條、第十一條、第十二條或第十三條規定。 三、違反第二十條第二項或第三項規定。 四、違反第二十七條第一項或未依第二項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。 五、<u>未依第二十七條之一第一項規定，執行個人資料保護影響評估。</u>	**第四十八條** 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰： 一、違反第八條或第九條規定。 二、違反第十條、第十一條、第十二條或第十三條規定。 三、違反第二十條第二項或第三項規定。 四、違反第二十七條第一項或未依第二項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。	配合本法新增第二十七條之一，增訂第四十八條第五款。

（二）如暫不於個資法中增訂強制執行個資保護影響評估之規範，可修正個資法施行細則，細部說明個資保護影響評估之適用情況、範圍、項目。修正條文草案對照表如下：

表 16、個資保護影響評估施行細則修正條文草案對照表

修正條文	現行條文	說明
第十二條之一 I 公務機關或非公務機關蒐集、處理或利用個人資料之行為，或該行為涉及之系統，依其性質、背景、目的與範圍，對當事人權益有高風險之虞者，前條第 2 項第 3 款之個人資料之風險評估，得包含個人資料保護影響評估，並於行為前或系統使用前為之。 II 前項所稱對當事人權益有高風險之虞，包含但不限於下列各款情形之一： 一、對當事人為評估或預測（包含剖析）。 二、具有法律效果或類似重大效果之自動化決策。 三、對當事人之系統性監控。 四、涉及本法第六條之	（本條新增）	為強化公務機關與非公務機關之問責性，課予機關事先識別其行為對個人資料當事人權益造成潛在風險之責任，俾使機關得事先採取各項風險因應措施，爰參考歐盟個人資料保護規則（GDPR）第 35 條規定，增訂第十二條之一關於個人資料保護影響評估之規範，落實機關之資料治理責任。

個人資料。 五、依涉及人數、資料數量、持續時間等條件，大規模蒐集、處理或利用個人資料。 六、匹配或組合不同資料集。 七、蒐集、處理或利用弱勢當事人之個人資料。 八、創新利用或應用新的技術性或組織性解決方案。 九、該行為之將阻止當事人行使權利、使用服務或締結契約。 III 第一項所稱個人資料保護影響評估，至少應包括下列事項： 一、識別蒐集、處理或利用個人資料之行為、範圍與流程。 二、檢視蒐集、處理或利用個人資料之合目的性與合比例性。 三、評估個人資料之風		

險。 四、規劃風險因應措施。 IV 公務機關或非公務機關應依個人資料保護影響評估結果，採取規劃之風險因應措施以避免或降低風險，並應持續監控剩餘風險，即時改善風險因應措施之有效性。		

（三）依前述修正之施行細則訂定指引草案（附件 4）

第六章　附件

附件 1：當事人拒絕利用個人資料行銷指引（草案）

當事人拒絕利用個人資料行銷指引（草案）	
草案	說明
一、本指引目的 （一）個人資料保護法（以下稱「本法」）為保障個人資料當事人免受行銷打擾之權益，於第二十條第二項及第三項分別規定「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」，明定當事人得對非公務機關利用個人資料之行銷行為表示拒絕。 （二）本指引就前揭當事人拒絕行銷之規定提供注意事項，俾利非公務機關利用個人資料行銷時之參考。	說明本指引目的，本指引係參考文件，無法律拘束力，亦不影響司法機關或各目的事業主管機關本於權責對個資法及施行細則之解釋與適用。
二、首次利用個人資料行銷之注意事項	個資法就非公務機關首次利用個人資料行銷定有較高義務，要求

（一）非公務機關首次利用個人資料行銷前，當事人已表示拒絕接受行銷者，非公務機關應尊重當事人意願，不得利用其個人資料行銷。 （二）非公務機關應向當事人告知得拒絕接受行銷，亦應提供當事人表示拒絕接受行銷之方式，並支付所需費用。 （三）如非公務機關以通話行銷者，行銷人員應於通話中清楚向當事人說明「如果不願再收到行銷通話，請告知」等類似語句。 （四）如非公務機關以簡訊行銷者，得於簡訊中提供拒絕接受行銷之電話專線，或告知當事人得向發出簡訊之電話號碼以簡訊回覆拒絕接受行銷。 （五）如非公務機關以電子郵件行銷者，得於電子郵件中提供當事人得回覆以拒絕接受行銷之電子郵件或其	向當事人提供表示拒絕行銷之方式，故針對不同行銷方式，提示優良實務做法。

他方式（例如：取消訂閱電子報之勾選框格）。 （六）如非公務機關以紙本郵寄或傳真行銷者，得提供當事人表示拒絕接受行銷之表格，並附上回郵信封供當事人寄回。	
三、當事人表示拒絕接受行銷時之注意事項 （一）當事人對非公務機關利用其個人資料行銷之行為，有權任意表示拒絕，不以非公務機關首次利用其個人資料行銷時為限。如非公務機關以當事人同意作為行銷之合法要件時，倘當事人表示撤回該同意，即等同拒絕接受行銷。 （二）當事人表達拒絕接受行銷之意時，非公務機關即應停止利用其個人資料行銷，其後亦不得再利用其個人資料行銷。 （三）如當事人未對非公務機關以特定個人資料之特定利用方式作為行銷管道（例如電話行銷、簡訊行銷、	個資法賦予當事人對利用其個資行銷行為之任意拒絕權，如當事人表示拒絕行銷，非公務機關即應停止利用個人資料行銷。故參考英國資訊委員辦公室（ICO）《行銷指引》與香港個人資料私隱專員公署《直接促銷新指引》，提示優良實務做法。

電子郵件行銷、郵寄通訊行銷）表示拒絕時，應視為拒絕所有利用個人資料行銷之行為。非公務機關得以適當方式，在不造成當事人過度侵擾之範圍內，確認當事人之真意。 （四）本法第二十條第三項雖對非公務機關課予義務，規範非公務機關須提供當事人表示拒絕接受行銷之方式，惟本法並未限制當事人僅得以非公務機關提供之方式表示拒絕接受行銷。 （五）非公務機關應採取適當的管理上或技術上措施，有效記錄並處理當事人對於利用其個人資料行銷之拒絕，確保當事人表達拒絕接受行銷之意能獲得滿足。前述措施得包含相應之作業流程管理程序，與具備相應功能之操作系統。	
四、當事人表示拒絕接受行銷後之注意事項	當事人對非公務機關表示拒絕行銷後，其拒絕效力應非以該單次行銷為限，故參考英國資訊委員

（一）非公務機關應以適當方式保存（例如：實體紙本、電子檔、系統資料庫）拒絕接受行銷之當事人名單。 （二）為確保管理之有效性，宜採取系統化方式記錄當事人提出拒絕接受行銷之表示，並應即時更新名單。 （三）非公務機關應採取適當之管理上或技術上措施，確保內部行銷業務相關人員取得當下正確之未拒絕接受行銷當事人名單。 （四）非公務機關如有各處營業據點或設有分公司（或其他類似同一法律主體關係）時，應採取適當之管理上與技術上措施，收集、統整並傳達即時、正確之拒絕接受行銷當事人名單。 （五）當事人表示拒絕非公務機關利用其個人資料行銷後，非公務機關即應檢視蒐集該當事人個人資料之特定目的是否仍存在，並	辦公室（ICO）《行銷指引》與香港個人資料私隱專員公署《直接促銷新指引》，提示落實當事人拒絕行銷請求之優良實務做法。

應依本法規定，主動或依當事人之請求，刪除、停止處理或利用特定目的已消失之個人資料（例如專為行銷目的蒐集之電子郵件信箱或收件地址）。	
五、其他注意事項 （一）如非公務機關委託他人利用個人資料向當事人行銷，應採取適當之監督措施（例如於雙方契約中納入對應約款），確保受託者依非公務機關之指示處理當事人拒絕行銷之請求。於此情形，當事人應有權選擇向受託者或委託之非公務機關表示拒絕接受行銷。 （二）多數非公務機關共同向當事人行銷其中一方或數方之商品或服務時（例如異業合作行銷活動），當事人向任一方表示拒絕接受行銷之意思時，除當事人有相反表示，應視為當事人拒絕接受所有非公務機關利用其個人資料行銷。接受當事人拒絕行銷意思	考量實務中委託他人行銷、合作行銷等情形，提示相關優良實務做法。

之該非公務機關，應即時通知其他非公務機關以記錄並更新行銷名單。	

附件 2：網路活動資料查詢閱覽權指引（草案）

網路活動資料查詢閱覽權指引（草案）	
草案	說明
一、前言 (一) 隨著網路應用日漸普及，民眾網路活動產生大量紀錄，其中相當部分得直接或間接識別從事網路活動之特定個人。為強化個人資料當事人之權益保障，個人資料保護法施行細則（以下稱細則）於 ooo 年 oo 月 oo 日增訂第四條第七項，明訂因網路活動產生或與之相關、得以直接或間接識別特定個人之資料，為個人資料保護法（以下稱本法）第二條第一款所稱之個人資料。 (二) 本指引就個人資料當事人如何就網路活動資料依本法請求查詢、閱覽，以及公務機關或非公務機關如何回應當事人權利行使提供說明，供相關各方參考。	說明本指引目的，本指引係參考文件，無法律拘束力，亦不影響司法機關或各目的事業主管機關本於權責對個資法及施行細則之解釋與適用。
二、網路活動資料 (一) **網路活動資料之含義**	一、 參酌歐盟 GDPR 第 4 條及前言第 30 點、美國加州《消費者隱私法》

1. 細則第四條第七項所稱之各類資料，合稱為網路活動資料。 2. 細則第四條第七項所稱之網路識別碼，包含 IP 位址、Mac 位址、cookie 或類似追蹤識別碼、使用者裝置識別碼、使用者帳號及名稱等。 3. 細則第四條第七項所稱之網路活動紀錄，包含登入、搜尋、點選、瀏覽、輸入、同步、匯出、刪除等網路活動之紀錄。 4. 細則第四條第七項所稱之基於網路活動而推知之資料，包含對該個人偏好、興趣、經濟狀況、行為、健康、位置、能力等特徵之分析、評估或預測。 5. 網路活動資料以間接方式識別該個人者，有效區分該個人與其他個人即足，不以獲知該個人之姓名或其實際身分為限。 **(二) 網路活動資料之管理**	（CCPA）第 v 項第 1 款等，提供網路活動資料之例示。 二、 因網路活動資料之性質較一般資料有顯著不同，參考英國 ICO《近用權指引》，就網路資料之儲存、保護、管理程序等提供優良實務做法。

1. 公務機關或非公務機關宜根據所涉網路活動資料之特徵，適當建置並維護資訊管理系統，並保留適足詮釋資料[388]。 2. 公務機關或非公務機關宜就所涉網路活動資料，執行盤點及清查，盤點項目包括種類、性質、儲存方式、儲存位置、保存期限、保護措施等； 3. 公務機關或非公務機關宜根據網路活動資料之特徵，就網路活動資料之蒐集、處理及利用訂定適當管理程序，包括： (1) 蒐集、處理及利用之適法性確認； (2) 蒐集、處理及利用之紀錄保存； (3) 資料保護措施之確定、執行與評估； (4) 資料保存期限之評估及期限屆滿後之處理；	

[388] 詮釋資料（Metadata）即描述資料的資料。惟應注意者，詮釋資料得以直接或間接識別特定個人時，屬個人資料，當事人得對其行使本法第 3 條規定的資料權利。

(5) 當事人權利行使請求之受理、審查及回應； (6) 相關人員之教育訓練。	
三、網路活動資料查閱請求 **(一) 查閱請求之提出** 1. 當事人得依本法第 3 條第 1 款及第 2 款、第 10 條，自行或透過代理人向蒐集、處理或利用其網路活動資料之公務機關或非公務機關，請求查詢、提供閱覽或製給複製本（以下稱網路活動資料查閱請求）。 2. 公務機關或非公務機關宜向當事人提供提出網路活動資料查閱請求之便利管道，告知請求回應時程、收費標準及其他應釋明之事項，並保留所受理請求之紀錄。公務機關或非公務機關宜建立適當程序，識別、記錄並回應當事人於前開管道之外提出之網路活動資料查閱請求。 3. 公務機關或非公務機關宜根據所涉網路活動資料之特徵，提供自動化管道，	一、 網路活動資料即係由當事人網路活動產生，則宜提供自動化方式，以便利當事人行使查閱權並降低蒐集機關之回應成本。但自動化查閱管道之提供，不應限縮當事人行使查閱權之方式。 二、 網路活動資料多係間接識別性資料，當事人行使查閱權，須先驗證其身分，故參考英國 ICO《近用權指引》，提供優良實務參考。

供當事人自行查詢、閱覽、匯出或下載其網路活動資料。 4. 當事人請求查閱網路活動資料時，表明查閱網路活動資料之意願即足，不以使用法律術語或援引本法條文為必要。公務機關或非公務機關得提供標準書表等，作為當事人網路活動資料查閱請求之參考。 5. 當事人對網路活動資料請求查詢、閱覽或製給複製本，不影響該當事人對該資料享有之肖像權、著作權或其他權利。 **(二) 當事人身分及查閱範圍之確認** 1. 公務機關或非公務機關應建立適當程序，及時合理確認提出網路活動資料查閱請求之當事人身分，不得無故遲延。當事人透過代理人提出網路活動資料查閱請求者，並應確認代理人之代理權。	

2. 公務機關或非公務機關提供帳號密碼登入驗證程序者，當事人依其程序登入帳號，應視為已確認身分，但公務機關或非公務機關有合理理由認為需進一步確認者，不在此限。 3. 公務機關或非公務機關宜建立適當程序，及時評估所受理之網路活動資料查閱請求，並於必要時請當事人確認或釐清請求內容或範圍。	
四、網路活動資料查閱請求之審查回覆 **(一) 查閱請求之審查** 1. 公務機關或非公務機關應建立適當程序，完整搜尋與彙整網路活動資料查閱請求所涉資料。搜尋範圍應涵蓋各系統、檔案、資料、記錄，包括相關備份，以及委託他人處理之資料。 2. 以現有資料不能識別當事人者，公務機關或非公務機關無須為回應當事人請	一、網路活動資料多係間接識別性資料，蒐集機關未必掌握足以識別當事人之全部資訊。故參考歐盟 GDPR 第 11 條與第 12 條，提供優良實務參考。 二、參考歐盟 GDPR、新加坡個人資料保護法（PDPA）、英國 ICO《近用權指引》等，提供優良實務參考。

求之唯一目的，蒐集、處理或利用該當事人之其他資料，但當事人為行使權利目的提供其他資料以實現識別者，不在此限。 **(二) 查閱請求之回覆** 1. 公務機關或非公務機關受理當事人網路活動資料查閱請求後，應於本法第 13 條所定時限內予以答覆。本法第 13 條所定時限，自公務機關或非公務機關確認當事人身分之日起算，因查閱請求範圍不明、現有資料無從識別當事人等情事，有必要與當事人溝通者，溝通所需時間不計入本法第 13 條所定時限。 2. 公務機關或非公務機關宜以當事人提出請求之相同方式回覆該請求，但當事人另有要求、或當事人提出請求之方式不適於回覆者，不在此限。 3. 公務機關或非公務機關經審查當事人網路活動資料查閱請求，核准提供查詢	

或閱覽者，宜向當事人提供線上查詢或閱覽方式。 4. 公務機關或非公務機關經審查當事人網路活動資料查閱請求，核准提供複製本者，宜向當事人提供複製本之遠端下載。 5. 網路活動資料查閱請求所涉網路活動資料作為文檔紀錄之一部者，公務機關或非公務機關得以節錄等方式提供該資料，無需提供完整文檔。 6. 查詢或請求閱覽網路活動資料或製給複製本者，公務機關或非公務機關得依本法第 14 條規定酌收必要成本費用。 7. 提供線上查詢、閱覽、傳輸複製本或提供下載，應採取加密等措施確保資訊安全。 (三) **查閱請求之拒絕**[389]	

[389] 當事人網路活動資料如屬《政府資訊公開法》所稱之政府資訊，應優先適用該法規定，即其提供亦可能有該法第 18 條第 1 項之限制情形（例如第 6 款「公開或提供有侵害個人隱私、職業上秘密或著作權人之公開發表權者。但對公益有必要或為保護人民生命、身體、健康有必要或經當事人同意者，不在此限」、第 7 款「個人、法人或團體營業上秘密或經營事業有關之資訊，其公開或提供有侵害該個人、法人或團體之權利、競爭地位或其他正當利益者。但對公益有必要或為保護人民生命、身體、健康有必要或經當事人同意者，不在此限。」等）。

1. 當事人之網路活動資料查閱請求有下列情形之一者，公務機關或非公務機關得拒絕當事人請求，並將其原因以書面通知當事人： (1) 該公務機關或非公務機關已不再持有請求所涉之網路活動資料； (2) 該公務機關或非公務機關無法確認當事人身分； (3) 該公務機關或非公務機關縱經當事人提供其他資料，亦無從以現有資料識別該當事人； (4) 其他事實上無法查詢、閱覽或製給複製本之正當事由。 2. 當事人之網路活動資料查閱請求有本法第 10 條但書所列情形之一者，公務機關或非公務機關應拒絕當事人請求並將其原因以書面通知當事人，但其妨害該蒐集機關之重大利益	

者，該蒐集機關得酌情決定核准該請求。 3. 本法第 10 條但書第 2 款所稱之妨害公務機關執行法定職務，包括違反公務機關依職權對蒐集該網路活動資料之非公務機關所作指示。 4. 本法第 10 條但書第 3 款所稱妨害該蒐集機關之重大利益，包括： (1) 妨害該蒐集機關之生命、身體、自由或其他人格權益之合理保護； (2) 妨害該蒐集機關營業秘密、智慧財產權或其他財產權益之合理保護； (3) 嚴重損害該蒐集機關之市場競爭地位或經營上之正當利益； (4) 當事人於短時間內反覆就相同資料一再提出請求，妨礙該蒐集機關之正常運作，且當事人對於該網路活動資料之查詢、閱覽或製給複製	

本，顯無更值得保護之重大利益。 (5) 提供查詢、閱覽或製給複製本將耗費該蒐集機關大量時間、勞力或費用，且當事人對於該網路活動資料之查詢、閱覽或製給複製本，顯無更值得保護之重大利益。 5. 本法第 10 條但書第 3 款及細則第 18 條所稱妨害第三人之重大利益，包括： (1) 妨害第三人之生命、身體、自由或其他人格權益； (2) 妨害第三人營業秘密、智慧財產權或其他財產權益之合理保護； (3) 該網路活動資料查閱請求所涉資料內包含第三人之個人資料，且無法以遮罩、節錄等方式予以分離者，但該第三人個人資料係由該當事人提供者，不在此限。	

6. 公務機關或非公務機關拒絕當事人網路活動資料查閱請求者，以請求所涉資料中存在事實上不能或本法第 10 條但書所列例外情事者為限，且應將拒絕原因以書面通知當事人。因本指引第(三).4.(5)之情事拒絕請求者，應在所耗時間、勞力及費用合理之範圍內，向當事人提供所請求網路活動資料之相關資訊。 7. 公務機關或非公務機關拒絕當事人網路活動資料查閱請求或未於本法規定期間內答覆者，當事人得依相關法律提起訴願或訴訟。	

附件 3：個資侵害事故通知當事人指引（草案）

個資侵害事故通知當事人指引（草案）	
草案	說明
一、 前言 (一) 為強化個人資料當事人之權益保障，個人資料保護法施行細則（以下稱細則）於 ooo 年 oo 月 oo 日修正第二十二條，明定個人資料被竊取、洩漏、竄改或其他侵害者，其依個人資料保護法（以下稱本法）通知當事人，如侵害所致當事人隱私及其他權利保護風險較低、或通知所需勞費過鉅，得以網際網路、新聞媒體或其他適當公開方式為之，以利保護當事人免受不必要的通知疲勞，並兼顧通知當事人之現實可行性。 (二) 本指引就個人資料侵害事故（以下稱個資侵害事故）通知當事人之執行提供說明，俾利公務機關或非公務機關參考。	說明本指引目的，本指引係參考文件，無法律拘束力，亦不影響司法機關或各目的事業主管機關本於權責對個資法及施行細則之解釋與適用。

二、 個資侵害事故 **(一) 個資侵害事故之含義** 1. 本指引所稱之個資侵害事故，係指本法第 12 條規定之個人資料遭竊取、洩漏、竄改或其他侵害之事故。 2. 本法第 12 條所稱之個人資料之其他侵害，包括因故意或過失，不當損害個人資料之機密性、完整性或可用性者，例如： (1) 因人為或技術原因，致使個人資料毀損或滅失； (2) 個人資料由未經授權之人存取使用； (3) 個人資料被不當公開或向未經授權之人揭露； (4) 載有個人資料之儲存裝置遺失、被竊或被劫持。 **(二) 個資侵害事故之識別與查明** 1. 公務機關或非公務機關應採取技術上及組織上之措	一、 參考歐盟GDPR關於個資侵害事故之定義，提供個資侵害事故之解釋。 二、 參考我國資通安全管理法、歐盟GDPR等規範，提供個資侵害事故識別與初步因應之優良實務做法。

施，監控個資保護狀況，偵測並及時提示個資侵害事故。相關措施得包括： (1) 存取權限管控及入侵警示機制； (2) 資料流與日誌分析與異常偵測機制； (3) 疑似個資侵害事故通報之內部程序； (4) 識別個資侵害事故之教育訓練； (5) 其他利於及時識別個資侵害事故之措施。 2. 公務機關或非公務機關於知悉資通安全事件或其他可能導致個資侵害之情事後，應立即採取措施確認個資侵害事故是否確已發生。確認發生個資侵害事故者，應立即查明其基本事項，並採取應變措施。應查明之基本事項包括： (1) 個資侵害事故之發生經過與性質； (2) 所涉個人資料之類型、內容、數量及狀態；	

(3) 所涉當事人之性質、範圍與數目； (4) 對於評估與因應個資侵害事故有重要影響之其他事項。	
三、 風險評估 (一) 公務機關或非公務機關發生個資侵害事故者，應基於所查明之事故基本事項，評估個資侵害事故對當事人隱私及其他權利之風險，並採取相應風險防範及損害補救措施。 (二) 對當事人隱私及其他權利之風險評估應以客觀標準進行，於個案中衡酌對當事人隱私、生命、健康、自由、財產、名譽等權利之潛在不利影響，以及該不利影響發生之可能性，評估之考量要素得包括： 1. 侵害事故之性質，例如侵害事故是否涉及個人資料遭竊取、洩露或由未經授權之第三人存取等； 2. 所涉個人資料之類型、內容及其敏感度或辨識性，	參考歐盟 GDPR、新加坡 PDPA、歐盟第 29 條個資工作小組（WP29）《個資侵害通知指引》等，提供個資侵害事故風險評估之優良實務做法及相關例示。

例如是否涉及本法第6條所列資料、身分證明資料或金融帳戶資料等； 3. 所涉個人資料之數量，例如是否涉及同一當事人之多筆資料等； 4. 所涉個人資料之狀態，例如資料是否已加密等； 5. 所涉當事人之性質，例如是否涉及未成年人等； 6. 已採取或得採取之因應措施，例如是否可立即有效恢復被損毀的資料等； 7. 對於風險評估有重要影響之其他要素。 (三) 公務機關或非公務機關經評估認定個資侵害事故對當事人隱私、生命、健康、自由、財產、名譽等權利之不利影響程度較低，或不利影響之發生可能性較低者，得認為事故所致當事人隱私及其他權利風險較低，其情形例如：	

1. 所涉個人資料之敏感度及辨識性較低，難以據此識別特定個人或作不當利用； 2. 所涉個人資料已加密或採取其他保護措施，且未經授權之人無法解讀其內容。 (四) 如個資侵害事故之發展變化或後續獲知之事實，對當事人隱私及其他權利之侵害風險有重大影響，公務機關或非公務機關應據此再次執行風險評估。	
四、 個資侵害事故通知當事人 **(一) 通知方式** 1. 公務機關或非公務機關發生個資侵害事故者，應於查明事故基本事項後，依本法第 12 條及細則第 22 條規定，以適當方式通知當事人。基本事項難以全部立即查明者，應就已查明部分先行通知當事人。通知宜使用簡明易懂之語言，以專門訊息方式為	個資侵害事故當事人之方式及內容，參考歐盟 GDPR、新加坡 PDPA、歐盟第 WP29《個資侵害通知指引》、日本個人資訊保護委員會《個人資訊保護法指引》等，提供確定適當通知方式及其內容之優良實務做法及相關例示。

之，以利當事人及時準確瞭解通知之性質與內容。 2. 依細則第 22 條第 1 項但書規定以公告方式為之者，應考量個資侵害事故所涉個人資料性質、隱私及其他權利之風險等要素，合理確定公告之管道、形式、期間等。 3. 公務機關或非公務機關基於所查明之事項依客觀標準執行風險評估，認為個資侵害事故所致當事人隱私及其他權利風險較低者，得依細則第 22 條第 1 項但書以網際網路、新聞媒體或其他適當公開方式向當事人為通知。但因個資侵害事故之發展變化或後續獲知之事實，使當事人隱私及其他權利保護風險提高者，公務機關或非公務機關宜以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或公告等適當方式，將個資侵害事故通知當事人。	

4. 細則第 22 條第 1 項但書所稱勞費過鉅，應衡酌個別通知當事人所需勞費成本、事故發生機關之負擔能力，以及個資侵害事故所致當事人隱私或其他權利風險綜合判斷，相關情形例如： (1) 因自始未蒐集或隨侵害事故遺失當事人聯絡資訊，而難以通知當事人； (2) 當事人數目眾多且聯絡資訊過於陳舊，而難以逐一查證更新； (3) 當事人數目眾多而無法以自動化方式聯絡，通知所需成本顯逾事故發生機關負擔能力。 (二) **通知內容** 1. 公務機關或非公務機關依本法第 12 條及細則第 22 條規定通知當事人，其內容宜包括：	

(1) 個資侵害事故之概述，例如事故性質、所涉個人資料內容等； (2) 個資侵害事故對當事人權益之可能影響； (3) 已採取及預計採取之因應措施； (4) 協助當事人防範不利影響之建議； (5) 當事人獲取更多資訊之聯絡窗口。 2. 依細則第 22 條第 1 項但書採公告方式通知者，其內容除前項所列外，並宜包括受影響之當事人範圍及當事人確認自身是否受影響之方法。	
五、 其他 (一) 公務機關或非公務機關委託他人蒐集、處理或利用個人資料時，應就個資侵害事故之識別、查明、風險評估及通知事宜為明確約定。 (二) 公務機關或非公務機關就個資侵害事故之發生、查	依據個資法委外監督義務、課責原則等，提示蒐集機關在因應個資侵害事故之其他優良實務做法。

明、風險評估及通知，應記錄其各項機制、程序、措施及判斷，並留存軌跡資料或相關證據。 (三) 公務機關或非公務機關依本法及細則因應及通知個資侵害事故，宜留意依資通安全管理法等其他法律規範之事故通知通報要求。	

附件 4：個人資料保護影響評估指引（草案）

個人資料保護影響評估指引（草案）	
草案	說明
一、 本指引目的 (一) 為強化個人資料當事人之權益保障，個人資料保護法施行細則於ooo年oo月oo 日修正增訂第十二條之一，明訂公務機關或非公務機關蒐集、處理或利用個人資料之行為，或該行為涉及之系統，依其性質、背景、目的與範圍，對當事人權益有高風險之虞者，該機關對個人資料之風險評估，應包含個人資料保護影響評估，並於行為前或系統使用前為之。 (二) 本指引就個人資料保護影響評估（以下稱個資保護影響評估）之執行提供說明，俾利公務機關或非公務機關參考。	說明本指引目的，本指引係參考文件，無法律拘束力，亦不影響司法機關或各目的事業主管機關本於權責對個資法及施行細則之解釋與適用。
二、 個資保護影響評估步驟	個資保護影響評估應以規劃之個資蒐集、處理或利用行為之實際步驟為評估對象，檢視該行為是

(一) 識別蒐集、處理或利用個人資料之行為、範圍與流程，至少包含下列事項： 1. 所規劃者屬蒐集、處理或利用個人資料之行為，及該行為之背景、目的與涉及之個人資料。 2. 該行為所涉個人資料之保存方式與期限。 3. 該行為涉及將個人資料提供予第三人（包含受機關委託之受託者）者，應敘明該第三人或其業別，及將個人資料提供予第三人之合法要件。 (二) 檢視蒐集、處理或利用個人資料之合目的性與合比例性，尤應檢視下列原則之遵循： 1. 該行為之目的應特定、明確、合法。 2. 該行為僅蒐集、處理或利用適當、相關且必要之個人資料。	否符合個資法之基本原則及各項具體規範，評估對當事人權益之影響，並採取風險規避或降低措施。故參考歐盟 GDPR、新加坡 PDPA、歐盟 WP29《DPIA 指引》、新加坡個人資料保護委員會《DPIA 指引》等，就評估各步驟之執行方式提示優良實務做法。

(三) 評估個人資料保護法之遵循性，至少包含下列事項： 1. 依個人資料保護法第 6 條、第 15 條、第 16 條、第 19 條、第 20 條規定，評估蒐集、處理與利用個人資料之合法要件。 2. 如以同意為蒐集、處理或利用個人資料之合法要件者，依個人資料保護法第 7 條規定，評估同意之合法性。 3. 依個人資料保護法第 8 條及第 9 條規定，評估告知義務之存否與踐行方式。 4. 依個人資料保護法第 11 條規定，評估個人資料之正確性維持與保存期限或保存條件。 5. 依個人資料保護法第 3 條、第 10 條、第 11 條、第 13 條規定，評估當事人權利行使之原則、例外及行使方式。 6. 非公務機關為國際傳輸個人資料者，檢視是否受中	

央目的事業主管機關依個人資料保護法第 21 條規定所為之限制。 7. 委託他人蒐集、處理或利用個人資料者，依個人資料保護法施行細則第 8 條規定，評估對受託者之監督。 8. 依個人資料保護法第 12 條規定，評估個人資料事故通知之機制。 (四) 鑑別個人資料之風險，至少應包含下列事項： 1. 以當事人權益受影響程度鑑別風險。 2. 依據前三項之識別、檢視與評估結果，鑑別風險種類與來源，並宜徵詢機關內外關係人（例如員工、受託者、接收個人資料之第三人）之意見。 3. 鑑別風險發生之可能性，以及風險發生對當事人權益影響之嚴重性。	

(五) 依據鑑別之風險，預先規劃足以避免或降低風險之因應措施。	
三、 個資保護影響評估結果 (一) 機關應將個資保護影響評估結果與決策作成紀錄。 (二) 機關應依個資保護影響評估結果，對該行為或涉及之系統，採取風險因應措施。 (三) 機關應持續監控剩餘風險，即時改善風險因應措施之有效性。	個資保護影響評之目的係協助因應個資蒐集、處理或利用行為對當事人權益之影響，故依據個資法課責原則，並考歐盟 GDPR、新加坡 PDPA、歐盟 WP29《DPIA 指引》、新加坡個人資料保護委員會《DPIA 指引》等，就評估結果之記錄與利用提示優良實務做法。

表 17、個人資料保護影響評估檢核表

個人資料保護影響評估檢核表		
編號	內容	
策略面		
1	機關已針對個資保護影響評估之執行訂定政策與程序。	□
2	機關理解如何識別何種條件須執行個資保護影響評估。	□
3	機關於內部提供認知訓練，培養同仁針對涉及蒐集、處理或利用個人資料的新行為或新系統，評估是否須執行個資保護影響評估之意識，以及執行之能力。	□

4	機關記錄並保存每次執行個資保護影響評估之結果與決策。	□
程序面		
5	機關之行為或系統如涉及蒐集、處理或利用個人資料而有下列情形時，即應考量執行個資保護影響評估： □ 對當事人為評估或預測（包含剖析） □ 具有法律效果或類似重大效果之自動化決策 □ 對當事人之系統性監控 □ 涉及個人資料保護法規定之特種個人資料 □ 依涉及人數、資料數量、持續時間等條件，屬大規模蒐集、處理或利用個人資料 □ 匹配或組合不同資料集 □ 蒐集、處理或利用弱勢當事人之個人資料 □ 創新利用或應用新的技術性或機關性解決方案 □ 該行為將阻止當事人行使權利、使用服務或締結契約	
6	如既有行為或系統之性質、範圍、內容或目的有變更時，機關將再次考量執行個資保護影響評估。	□
7	如經考量不執行個資保護影響評估，機關將記錄該決定之原因。	□
執行面		
8	確認屬於蒐集、處理或利用個人資料之行為，及該行為之背景、目的與涉及之個人資料。	□
9	確認個人資料之保存方式與期限。	□
10	如將個人資料提供予第三人（包含受機關委託之受託者）者，應識別該第三人或其業別。	□
11	檢視目的是否特定、明確、合法。	□
12	檢視是否僅蒐集、處理或利用適當、相關且必要之個人資料。	□
13	評估蒐集、處理與利用個人資料之合法要件。	□

14	評估同意之合法性（如有需要）。	□
15	評估告知義務之存否與踐行方式。	□
16	評估個人資料之正確性維持與保存期限或保存條件。	□
17	評估當事人權利行使之原則、例外及行使方式。	□
18	如機關為非公務機關而有意國際傳輸個人資料者，檢視中央目的事業主管機關之限制。	□
19	委託他人蒐集、處理或利用個人資料者，評估對受託者之監督。	□
20	評估個人資料事故通知機制。	□
21	以當事人權益受影響程度鑑別風險。	□
22	鑑別風險種類與來源，並徵詢機關內外關係人之意見。	□
23	鑑別風險發生之可能性，以及風險發生對當事人權益影響之嚴重性。	□
24	依據鑑別之風險，預先規劃足以避免或降低風險之因應措施。	□
25	依據個資保護影響評估結果，對該行為或涉及之系統，採取規劃之風險因應措施。	□
26	持續監控剩餘風險，即時改善風險因應措施之有效性。	□

第七章　參考資源

法律規範

1、歐盟法規

(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
(2) Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

2、美國法規

(3) California Civil Code, Division 3, Part 4, Title 1.81 (Customer Records).
(4) California Consumer Privacy Act of 2018 (California Civil Code, Division 3, Part 4, Title 1.81.5).
(5) California Consumer Privacy Act Regulations (California Code of Regulations, Title 11, Division 1, Chapter 20.
(6) California Privacy Rights Act of 2020 (Initiative Proposition 24).
(7) Code of Virginia, Title 18.2, Chapter 6, Article 5 (False Representations to Obtain Property or Credit).
(8) Gramm-Leach-Bliley Act (GLBA) Regulations (16 CFR Part 314).
(9) Health Insurance Portability and Accountability Act (HIPAA) administrative simplification (45 CFR Parts 160, 162, and 164).
(10) Virginia Consumer Data Protection Act (Code of Virginia, Title 59.1, Chapter 53).

3、日本法規

(11) 個人情報の保護に関する法律（平成十五年法律第五十七号，令和二年法律第四十四号による改正）。

(12) 行政機関の保有する個人情報の保護に関する法律（平成十五年法律第五十八号，令和元年法律第三十七号による改正）。

(13) 行政機関の保有する情報の公開に関する法律（平成十一年法律第四十二号，平成二十八年法律第五十一号による改正）。

(14) 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成二十五年法律第二十七号，令和三年法律第十一号による改正）。

(15) 独立行政法人等の保有する個人情報の保護に関する法律（平成十五年法律第五十九号，令和元年法律第三十七号による改正）。

(16) デジタル社会の形成を図るための関係法律の整備に関する法律（令和三年法律第三十七号）。

(17) 個人情報の保護に関する法律施行令（平成十五年政令第五百七号，令和三年政令第五十六号による改正）。

(18) 個人情報の保護に関する法律施行規則（平成二十八年個人情報保護委員会規則第三号，令和三年個人情報保護委員会規則第一号による改正）。

(19) 特定個人情報保護評価に関する規則（平成二十六年特定個人情報保護委員会規則第一号，令和三年個人情報保護委員会規則第三号による改正）。

4、韓國法規

(20) 개인정보보호법，[법률 제 16930 호, 2020. 2. 4., 일부개정].

(21) 개인정보보호법시행령，[대통령령 제 30892 호, 2020. 8. 4, 일부개정].

5、 新加坡法規

(22) Personal Data Protection Act 2012 (Act 26 of 2012, Amended by Act 40 of 2020).
(23) Personal Data Protection Regulations 2021 (SL 63/2021).
(24) Personal Data Protection (Notification of Data Breaches) Regulations 2021 (SL 64/2021).

司法判決

(25) Court of Justice of the European Union (CJEU), Patrick Breyer v Bundesrepublik Deutschland (Case C‑582/14), Judgment of 19 October 2016.

實務指引與工作文件

1、 我國

(26) 臺灣開放政府國家行動方案：2021 年至 2024 年（2021 年 1 月）。
(27) 金融監督管理委員會民國 101 年 10 月 24 日金管銀合字第 10130002690 號函。
(28) 法務部民國 101 年 12 月 10 日法律字第 10103107080 號函。
(29) 法務部民國 102 年 3 月 12 日法律字第 10100271950 號函。
(30) 法務部民國 104 年 8 月 20 日法律字第 10403510420 號函。
(31) 法務部民國 104 年 10 月 23 日法律字第 10403513240 號函。
(32) 法務部民國 105 年 11 月 11 日法律字第 10503515840 號函。
(33) 法務部民國 106 年 1 月 26 日法律字第 10503517710 號函。
(34) 法務部民國 106 年 6 月 5 日法律字第 10603503230 號函。
(35) 法務部民國 107 年 5 月 15 日法律字第 10703506760 號函。
(36) 法務部民國 107 年 7 月 3 日法律字第 10703507550 號函。

(37) 法務部民國 107 年 9 月 5 日法律字第 10703513330 號函。
(38) 法務部民國 107 年 5 月 15 日法律字第 10703506760 號函。
(39) 國家發展委員會民國 107 年 11 月 11 日發法字第 1072002136 號函。
(40) 國家發展委員會民國 108 年 1 月 22 日發法字第 1080000958 號函。
(41) 國家發展委員會民國 108 年 3 月 12 日發法字第 1082000384 號函。
(42) 國家發展委員會民國 109 年 07 月 24 日發法字第 1090015912 號函。
(43) 國家人權行動計畫（初稿）（1091029 公聽會版本）。
(44) 監察院民國 109 年 1 月 16 日 109 教調 0004 號調查報告。

2、歐盟

(45) Article 29 Data Protection Working Party (WP29), Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (6 February 2018).
(46) European Commission, Data Protection as A Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation (COM(2020) 264 final, 24 June 2020).
(47) European Data Protection Board (EDPB), Guidelines 3/2019 on Processing of Personal Data through Video Devices (10 July 2019).
(48) EDPB, Guidelines 05/2020 on Consent under Regulation 2016/679 (4 May 2020).
(49) WP29, 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 (4 October 2017).
(50) WP29, Guidelines on Data Protection Officers ('DPOs') (5 April 2017).
(51) WP29, Guidelines on Personal Data Breach Notification under Regulation 2016/679 (6 February 2018).

3、日本

(52) 個人情報保護委員会，個人情報の保護に関する法律についてのガイドライン（通則編）（令和 3 年 1 月一部改正）。
(53) 個人情報保護委員会，特定個人情報保護評価指針（平成二十六年特定個人情報保護委員会告示第四号，令和 3 年個人情報保護委員会告示第 1 号による改正）。
(54) 個人情報保護委員会，個人データの漏えい等の事案が発生した場合等の対応について（平成 29 年個人情報保護委員会告示第 1 号）。

4、韓國

(55) 개인정보보호위원회 ，「 개인정보 보호법 」일부개정법률（안）입법예고（2021.01.06）.
(56) 개인정보보호위원회 ，디지털 시대 「 개인정보 보호법 」개정안 국회제출（2021.09.28）.

5、新加坡

(57) Personal Data Protection Commission (PDPC), Advisory Guidelines on Key Concepts in the PDPA (1 October 2021).
(58) PDPC, Guide on Managing and Notifying Data Breaches Under the PDPA (15 March 2021).
(59) PDPC, Guide to Managing Data Breaches (8 May 2015).
(60) PDPC, Guide to Managing Data Breaches 2.0 (22 May 2019).

學術研究資料

(61) 范姜真媺、周逸濱（2019），《日本個人資料保護相關法制之匿名（非識別）加工研究委託研究計畫結案報告》，國家發展委員會委託研究報告。

(62) 葉奇鑫（2019），《GDPR 相關指引文件研析委託研究計畫結案報告》，國家發展委員會委託研究報告。
(63) 葉奇鑫（2020），《韓國個人資料保護法制因應 GDPR 施行之調適委託研究計畫結案報告》，國家發展委員會委託研究報告。
(64) 張陳弘（2021），〈科技智慧防疫與個人資料保護：陌生但關鍵的資料保護影響評估程序〉，《臺大法學論叢》，50 卷 2 期，頁 337-400。
(65) 張陳弘（2021），《GDPR 施行兩周年評估報告之分析及相關議題研析委託研究計畫結案報告》，國家發展委員會委託研究報告。
(66) 郭戎晉（2020），〈從個人資料保護立法談 cookie 之定位、應用爭議與規範課題〉，《東吳法律學報》，32 卷 1 期，頁 69-104。

網路資料

(67) California Privacy Protection Agency, Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 (September 22, 2021), https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf.
(68) California Privacy Protection Agency Board, Meeting Materials (June 14, 2021), https://cppa.ca.gov/meetings/materials/20210614.pdf.
(69) James Denvil & Arielle Brown, CPRA Countdown: Changes to the Definition of "Personal Information" (29 January 2021), https://www.engage.hoganlovells.com/knowledgeservices/news/countdown-to-the-california-privacy-rights-act-changes-to-the-definition-of-personal-information.
(70) Lee & Ko, Proposed Amendments to the Personal Information Protection Act (March 5, 2021),

https://www.legal500.com/developments/thought-leadership/proposed-amendments-to-the-personal-information-protection-act/.

(71) UK Information Commissioner's Office, When can we refuse to comply with a request?, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/when-can-we-refuse-to-comply-with-a-request/.

附錄一 期中報告審查會議紀錄

「強化數位隱私保障所涉個人資料保護法相關議題研析」委託研究計畫期中報告審查會議紀錄

壹、會議時間：110年8月13日（星期五）上午10時

貳、會議地點：U Meet 網路視訊會議

參、主席：楊參事淑玲

肆、出（列）席人員：(詳後附名單)　　紀錄：陳韻如

伍、主席致詞：(略)

陸、報告事項：達文西個資暨高科技法律事務所（略）

柒、發言要點：(依發言順序排列)

一、東海大學法律學院范姜教授真媺

(一)報告第 8 頁提及日本國會於 2021 年 5 月通過的「數位社會建構規劃相關法律發展法」，該法律名稱的意思係為謀求數位化社會形成而對相關法律整備之法律，建議此法律名稱翻譯再為修正；該法律於 2021 年 5 月通過，連帶將日本個人資料保護法一併進行修正，報告中提及的法律條文建議更新，例如數位足跡相關規定(如：cookie)，於日本修正後個人資料保護法中有相關規定，建議補充說明。

(二)報告中第 3 章第 1 節所述「對於公務機關執行法定職務之拒絕權」部分，提及「優勢公益」之舉證責任，惟由行政法觀點，人民倘主張公務機關未依法行政，本即應由公務機關負舉證之責，此處是否再賦予人民拒絕權，要求公務機關負舉證責任，建議再予以評估。

(三)報告第 107 頁關於「查閱權」部分，提及「日本個資法律則係以『提供』個人資料作為滿足當事人查閱權之方式」，其中「提供」應為揭露之意；揭露方式也於修法後，由「得以電子或書面方式提供」改為「得以依當事人指示方式提供」，建議於報告中補充。

(四)報告中第 3 章第 6 節個資衝擊影響評估，建議如要提案引進此政策，需考量企業規模、處理的個資性質種類、風險大小、企業成本與能力。

(五)日本公平會對網路科技業者（Google、Amazon、Facebook、Apple 等）之同意內涵曾發布指引，討論權力不對等、真心同意等問題，建議一併參考。

二、中國文化大學法律學系李教授寧修

(一)對報告之整體建議：建議可將簡報關鍵字、章節安排等納入報告；建議以表格方式，於各個議題最後增加法規比較，以輔助文字說明，較為清晰。短時間以制定指引或修改命令為因應方式，但宜於最後研究成果中呈現長期修法建議。建議在引用非英文之國外法規條文（尤其韓國）時，以中文翻譯呈現於報告中，助於理解。

(二)報告第 4 頁註腳 3 所提「個資衝擊影響評估」應屬誤植，建議改為「個資保護官」；報告第 3 章第 1 節當事人拒絕權，建議具體提出當事人拒絕權例外限制的情形為何，以及當事人就蒐集機關主張限制其拒絕權時之救濟方式。

(三)報告第 3 章第 4 節個資外洩通知，建議補充公務機關於個資侵害通報義務上所負的責任為何與作法。個資外洩通知與第 3 章第 6 節之 DPIA 均強調風險，建議補充說明風險高低標準應由誰判斷。

(四)報告第 3 章第 5 節當事人同意，書面同意難度較高，建議考量是否一併提及書面同意方式可於個資法上如何調整。

(五)報告第 3 章第 7 節個資保護官，參考衛生福利部現有資通安全治理暨個人資料保護會，其中資通安全暨個資保護長類似於資安長的職位。如公務機關普遍有類似資安長的職位，建議評估是否對於個資保護官的法規調適，能與現行制度結合，或調整擴充其職務。

三、政治大學法學院劉教授定基

(一)報告中有連動關係的議題，例如當事人同意與拒絕權，建議補充說明關聯性，較不會有不一致的情況；又例如報告第 25 頁在「拒絕權」部分，提及維吉尼亞州 CDPA 中，消費者有拒絕剖析的權利，但第 122 頁關於「自動化決策的告知義務」段落中，說明 CDPA 並無當事人得拒絕自動化決策之規定。建議釐清「剖析」與「自動化決策」的關係，避免報告前後敘述不一致。

(二)報告第 3 章第 1 節當事人拒絕權：

1. 第 18 頁提及歐盟 GDPR 關於「拒絕權」之規定，條文包含「當事人依其個案情形，有權拒絕處理其個人資料」，建議參考 EDPB 與 EDPS 近兩年針對科學研究及臨床實驗等指引，分析歐盟是否就「個案情形」提出解釋或示例。

2. 歐盟 GDPR 第 22 條雖列於「當事人權利」章節，但相關文獻似多將此一規定解釋為「禁止規定」(除例外情形，禁止為自動化決策)，建議點出此爭議，增加報告完整性。

3. 公務機關在「執行法定職務必要範圍內」是否還須提供當事人拒絕權？是否會增加公務機關之負擔？已具備蒐集處

理要件，再提供拒絕權是否會過於保護當事人？建議再予以評估。

4. 報告內對「拒絕權」之修法建議，方向為就現有蒐集、處理或利用個資之合法要件增列當事人拒絕權，但就現行個資法中不適宜的合法要件(例如對當事人權益無侵害、有利於當事人權益之要件)，應評估是否建議刪除，而非以賦予當事人拒絕權作為替代。

(三)報告第 96 頁中的「查閱權」部分，提及韓國個資法上的「輕易結合(間接識別)」概念，此一概念的具體內涵為何？如為報告中所述因為是輕易結合，數位足跡不一定包含在內，是否跟GDPR有實質上的不同？若如此，韓國為何能通過歐盟適足性認定？建議稍作補充。

(四)報告第 118 頁對歐盟 GDPR 中的「further process」，翻譯為「進階處理」，建議翻譯為我國常用之「目的外利用」或「與原始目的不同的處理」，或較為精確。

(五)報告第 119 頁提及之歐盟 GDPR 第 22 條自動化決策告知義務部分，在告知的內容上，學理及實務上似存有爭議，亦即告知範圍是否包含在決策作成「後」，向當事人告知作成決策之原因？就此，GDPR 第 22 條未明文規定，但 GDPR 前言第 71 點卻有提及，因而產生是否具法律拘束力的爭議？建議於報告中一併評估。

(六)報告第 211 頁提到「同意」的特定性，實務操作上如科學研究之同意可否放寬？醫學實驗上廣泛同意(broad consent)是否可被 GDPR 接受？GDPR 前言第 33 點似乎有放寬的空間，建議參考 EDPB、EDPS 等相關文獻，略為補充。

(七)報告第 3 章第 6 節個資衝擊影響評估，建議補充說明 DPIA 與我國現行個資法施行細則第 12 條的安全措施之差異。

四、法制協調中心

建議於報告中適當補充 2 次 OGP 座談會的專家學者意見。

五、研究團隊回應

(一)將於報告中更新日本最新條文、韓文條文改為中文翻譯呈現、增加關聯式敘述文字、各國法規比較表格等。

(二)書面同意部分建議搭配電子簽章法；公務機關個資事故通報建議沿用既有的資通安全管理法之通報機制，雖然資安與個資有所不同，但多為重疊，建議使用相同機制。

捌、 會議結論：

感謝與會者今日參與並提供寶貴意見，請研究團隊將委員所提相關意見納入後續期末報告修正。

散會（上午 11 時 30 分）

附錄二 期中審查意見回應說明

「強化數位隱私保障所涉個人資料保護法相關議題研析」

委託研究計畫期中審查意見回應說明

委員	編號	建議	研究團隊回應
范姜教授真媺	1	報告第 8 頁提及日本國會於 2021 年 5 月通過的「數位社會建構規劃相關法律發展法」，該法律名稱的意思係為謀求數位化社會形成而對相關法律整備之法律，建議此法律名稱翻譯再為修正；該法律於 2021 年 5 月通過，連帶將日本個人資料保護法一併進行修正，報告中提及的法律條文建議更新，例如數位足跡相關規定(如：cookie)，於日本修正後個人資料保護法中有相關規定，建議補充說明。	依委員建議調整為「數位社會整備法」，補充關於「個人關聯資訊」並於期末報告檢視該法連動調整之日本個人資訊保護法條文。
	2	報告中第 3 章第 1 節所述「對於公務機關執行法定職務之拒絕權」部分，提及「優勢公益」之舉證責任，惟由行政法觀點，人民倘主張公務機關未依法行政，本即應由公務機關負舉證之責，此處是否再賦予人民拒絕權，要求公務機關負舉證責任，建議再予以評估。	依委員建議於期末報告補充評估賦予當事人對公務機關執行法定職務之行為行使拒絕權之必要性。
	3	報告第 107 頁關於「查閱權」部分，提及「日本個資	依委員建議調整與補充於期末報告（第三

		法律則係以『提供』個人資料作為滿足當事人查閱權之方式」，其中「提供」應為揭露之意；揭露方式也於修法後，由「得以電子或書面方式提供」改為「得以依當事人指示方式提供」，建議於報告中補充。	章第二節第三目第四點之2）。
	4	報告中第3章第6節個資衝擊影響評估，建議如要提案引進此政策，需考量企業規模、處理的個資性質種類、風險大小、企業成本與能力。	依委員建議於期末報告綜合考量，擬於修法草案中授權由中央目的事業主管機關評估監理事業之特性，指定應執行個資保護影響評估之業務。
	5	日本公平會對網路科技業者（Google、Amazon、Facebook、Apple 等）之同意內涵曾發布指引，討論權力不對等、真心同意等問題，建議一併參考。	依委員建議納入期末報告（註270）。
李教授寧修	1	對報告之整體建議：建議可將簡報關鍵字、章節安排等納入報告；建議以表格方式，於各個議題最後增加法規比較，以輔助文字說明，較為清晰。短時間以制定指引或修改命令為因應方式，但宜於最後研究成果中呈現長期修法建議。建議在引用非英文之國外法規條文（尤其韓國）時，以中文翻譯呈現於報告中，助於理解。	依委員建議補充；為求慎重，增補韓國個資保護委員會官方版本之法規英譯連結。
	2	報告第4頁註腳3所提「個資衝擊影響評估」應屬誤植，建議改為「個資保護官」；報告第3章第1節當	依委員建議更正誤植處；並於期末報告提

		事人拒絕權，建議具體提出當事人拒絕權例外限制的情形為何，以及當事人就蒐集機關主張限制其拒絕權時之救濟方式。	出之修正草案中納入委員意見。
	3	報告第 3 章第 4 節個資外洩通知，建議補充公務機關於個資侵害通報義務上所負的責任為何與作法。個資外洩通知與第 3 章第 6 節之 DPIA 均強調風險，建議補充說明風險高低標準應由誰判斷。	依委員建議補充於期末報告（第三章第四節第二目第二點、第三章第四節第五目、第三章第六節第五目）。
	4	報告第 3 章第 5 節當事人同意，書面同意難度較高，建議考量是否一併提及書面同意方式可於個資法上如何調整。	現行個資法僅於第 6 條第 1 項但書第 6 款（對於特種個資之蒐集、處理與利用），以及第 11 條第 2 項但書（資料正確性有爭議時，得經當事人書面同意，並經註明其爭議而繼續處理或利用）、第 11 條第 3 項但書（特定目的消失或期限屆滿時，得經當事人書面同意，繼續保存、處理或利用），對當事人同意仍保留「書面」之要式要求，並可依電子簽章法規定，以電子文件為之。 考量本法於 104 年修正時已對書面同意之要式性通盤考量並修正，加以本研究議題著重同意之特性，是

			本研究擬暫不處理關於書面同意之爭議。
	5	報告第 3 章第 7 節個資保護官，參考衛生福利部現有資通安全治理暨個人資料保護會，其中資通安全暨個資保護長類似於資安長的職位。如公務機關普遍有類似資安長的職位，建議評估是否對於個資保護官的法規調適，能與現行制度結合，或調整擴充其職務。	依委員建議於期末報告納入評估（第三章第七節第五目）。
劉教授定基	1	報告中有連動關係的議題，例如當事人同意與拒絕權，建議補充說明關聯性，較不會有不一致的情況；又例如報告第 25 頁在「拒絕權」部分，提及維吉尼亞州 CDPA 中，消費者有拒絕剖析的權利，但第 122 頁關於「自動化決策的告知義務」段落中，說明 CDPA 並無當事人得拒絕自動化決策之規定。建議釐清「剖析」與「自動化決策」的關係，避免報告前後敘述不一致。	於第三章「研究發現」第一節「當事人拒絕權」第一項「議題釐清」中說明同意與拒絕權之關聯。 依委員建議於期末報告調整、補充。

	2	報告第 3 章第 1 節當事人拒絕權： (1) 第 18 頁提及歐盟 GDPR 關於「拒絕權」之規定，條文包含「當事人依其個案情形，有權拒絕處理其個人資料」，建議參考 EDPB 與 EDPS 近兩年針對科學研究及臨床實驗等指引，分析歐盟是否就「個案情形」提出解釋或示例。 (2) 歐盟 GDPR 第 22 條雖列於「當事人權利」章節，但相關文獻似多將此一規定解釋為「禁止規定」(除例外情形，禁止為自動化決策)，建議點出此爭議，增加報告完整性。 (3) 公務機關在「執行法定職務必要範圍內」是否還須提供當事人拒絕權？是否會增加公務機關之負擔？已具備蒐集處理要件，再提供拒絕權是否會過於保護當事人？建議再予以評估。 (4) 報告內對「拒絕權」之修法建議，方向為就現有蒐集、處理或利用個資之法律依據增列當事人拒絕權，但就現行個資法中不適宜的法律依據(例如對當事人權益無侵害、有利於當事人權益之要件)，應評估是否建議刪除，而非以賦予	依委員建議於期末報告補充；並評估賦予當事人對公務機關執行法定職務之行為行使拒絕權之必要性。 又委託機關已於另案研究現行個資法下，蒐集、處理或利用個資之合法要件的妥當性，是本案擬仍聚焦於當事人權利之研究需求。

		當事人拒絕權作為替代。	

	3	報告第 96 頁中的「查閱權」部分，提及韓國個資法上的「輕易結合(間接識別)」概念，此一概念的具體內涵為何？如為報告中所述因為是輕易結合，數位足跡不一定包含在內，是否跟 GDPR 有實質上的不同？若如此，韓國為何能通過歐盟適足性認定？建議稍作補充。	韓國個資法對於「輕易結合」並無明確定義，而是提出相關考量要素，於個案中具體判斷（見報告第三章第二節第三目的六點之 2）。歐盟 GDPR 所稱之間接識別，應仍考量控管者「合理可用」之識別手段（前言第 26 點），故韓國個資法與歐盟 GDPR 關於間接識別之定義，應係寬嚴標準不同，並無實質差異。又韓國取得歐盟適足性認定後，司法實務中會否將「輕易結合」作廣泛解釋，有待觀察。
	4	報告第 118 頁對歐盟 GDPR 中的「further process」，翻譯為「進階處理」，建議翻譯為我國常用之「目的外利用」或「與原始目的不同的處理」，或較為精確。	依委員建議調整，說明於註 149。
	5	報告第 119 頁提及之歐盟 GDPR 第 22 條自動化決策告知義務部分，在告知的內容上，學理及實務上似存有爭議，亦即告知範圍是否包含在決策作成「後」，向當事人告知作成決策之原因？就此，GDPR 第 22 條未明文規定，但 GDPR 前言第 71 點卻有提及，因而產生是否具法	依委員建議補充於註 154。

		律拘束力的爭議？建議於報告中一併評估。	
	6	報告第 211 頁提到「同意」的特定性，實務操作上如科學研究之同意可否放寬？醫學實驗上廣泛同意(broad consent)是否可被 GDPR 接受？GDPR 前言第 33 點似乎有放寬的空間，建議參考 EDPB、EDPS 等相關文獻，略為補充。	依委員建議補充於註 259。
	7	報告第 3 章第 6 節個資衝擊影響評估，建議補充說明 DPIA 與我國現行個資法施行細則第 12 條的安全措施之差異。	已於報告第三章「研究發現」第六節「個資保護影響評估」第四項「法規比較」章節比較差異，並依委員建議補充於註 353。

附錄三 期末報告審查會會議紀錄

「強化數位隱私保障所涉個人資料保護法相關議題研析」委託研究計畫期末報告審查會議紀錄

壹、會議時間：110年11月18日（星期四）上午9時30分

貳、會議地點：本會法制協調中心1樓會議室（實體及視訊方式）

參、主席：楊參事淑玲

肆、出（列）席人員：（詳後附名單）　　紀錄：陳韻如

伍、主席致詞：（略）

陸、報告事項：達文西個資暨高科技法律事務所（略）

柒、發言要點：（依發言順序排列）

一、 東海大學法律學院范姜教授真媺

（一）有關日本文獻翻譯用詞部分：

1. 日文中「者」與「事業」為不同概念，報告第 29 頁「個人資料處理者」與第 93 頁「個人資訊處理事業」，建議統一用詞使用「事業」。

2. 報告第 29 頁日文條文原文中無「滿足」二字，建議更精確翻譯原文。

3. 報告第 38 頁引用之日本個人資訊保護法條文應為第 30 條第 5 項，建議修正。

4. 報告第 95 頁「個人關連情報」中「情報」二字為日文用語，建議修正為「個人關連資訊」。

(二)日本行政機關個人資訊保護法的查閱權為避免與政府資訊公開法之規定衝突，故將得拒絕查閱的事由與政府資訊公開法為相

同規定。建議可參考日本作法，避免不同法規適用競合產生衝突。

(三)各國之 DPIA 規定有不同立法政策，且需考量公務或非公務機關的規模、性質、風險、接觸人數等因素，日本尚有「預備評估」、「略式評估」規定，建議做深入分析，釐清立法政策、適用對象、實施方式及利弊得失，再做進一步政策分析。

(四)報告第 126 頁標題「目的外利用與利用開放資料為自動化決策之告知」易造成混淆，不清楚是「目的外利用的告知」或是「利用開放資料為自動化決策」，且若以現行目的外利用的合法事由決定是否為目的外利用的告知較不恰當；另外，自動化決策的告知分為兩種，第一為告知當事人會做自動化決策，第二為告知當事人自動化決策的基準、運算邏輯與對其權利之影響，建議分開論述。

(五)有關個資侵害事故通知當事人，報告第 198 頁建議宜以對當事人權益有「高風險」者作為通知的標準，請補充關於「高風險」的定義。

(六)報告第 59 頁拒絕權的公益條款，報告所提依其立法理由似專為新聞業者而生，但是否僅有新聞報導符合公共利益，尚有疑義，建議刪除相關論述，避免爭議。

二、政治大學法學院劉教授定基

(一)報告第 46 頁有關公務機關執行法定職務必要範圍內，因目前法定職務的範圍(包括組織法、法規命令)，相較於歐盟 GDPR 的規定有些不同，或可作為賦予當事人拒絕權的理由。

(二)報告第 51 頁參考法務部的函釋，論述「當特種個人資料經過提供者處理後已無從識別當事人時，公務機關或學術研究機構取得的資料已非個人資料」，因該函釋尚有爭議，作為賦予學

術條款拒絕權的理由較不合適，建議改為參考國外立法例作為理由。

(三)報告第 85 頁所提由業者自動記錄之數位足跡，是否構成「自消費者取得」的特定個人資訊並適用資訊提供格式要求，似有討論空間等語，建議參考 CCPA 的相關文獻，予以補充。另外建議補充 CCPA 此條規定與第 130 頁所提及 CCPA 有關自動化決策，二者之關聯性為何？

(四)報告第 201 頁的結論，對於外洩通知檢討之範圍似乎過窄，建議呈現比較法的差異，例如：「查明後」之文字是否需刪除、是否增加通知期限規定等事項。

(五)報告第 235 頁關於當事人同意，未納入 GDPR 第 7 條內容的原因為何？若以特定性作為要件，是否包括禁止綑綁同意，似乎不夠明確；參考 GDPR 第 7 條第 2 項規定與其他意思表示應清楚區別之單獨同意，作為同意基本要件，而我國個資法僅有目的外利用有單獨同意的規定，是否需要增訂相關規定，建議於報告中說明，若不增訂，亦請說明不增訂的理由。

(六)報告第 263、264 頁將 DPIA 的風險分類為因應安全風險與因應當事人權益風險之評估，惟區分標準是否妥適，例如報告將 GDPR 之 DPIA 歸類為因應當事人權益風險之評估，但其似乎亦有包含因應安全風險之評估，建議補充說明分類之理由。

(七)修正條文之體例，建議再為整體評估；體例部分之修正，建議如下：

1. 報告第 303 頁個資法施行細則第 4 條第 7 項修正條文因為與現行個資法施行細則第 3 條都是涉及間接識別個資的定義，建議整併。

2. 報告第 304 頁個資法第 9 條之 1 修正條文告知義務與現行個資法第 8 條大致相同，建議整併至現有規定。報告第 306 頁個資法施行細則第 16 條第 2 項修正條文僅有在目的外利用才有「不能或需勞費過鉅始能向當事人或其法定代理人為告知」，為何在一般告知無相關規定，建議補充說明理由。

3. 報告第 309 頁個資法第 14 條之 1 修正條文有關同意的規定，是否需將所有同意條款列出，共通要件或許改為「本法所稱同意」即可。

(八)修正條文草案及指引實質內容之修正建議如下：

1. 第 299 頁個資法第 11 條第 5 項第 2 款修正條文「且資料未經提供者處理至無從識別特定之當事人」，現行法的問題對於「無從識別特定當事人」之定義尚有爭議，建議參考報告中對於查閱權之研究，於蒐集機關無對照組合資料得識別當事人之情形，蒐集機關並無義務為滿足當事人之請求而使用額外資訊為識別特定個人。

2. 報告第 307 頁個資法施行細則第 16 條之 1 修正條文「向當事人告知該個人資料之蒐集目的與利用方式」，已經是現行個資法第 8 條規定之範圍，修正條文用語無法呈現額外應告知之事項，建議增加告知自動化決策涉及的邏輯與效果。

3. 報告第 308 頁個資法第 12 條修正條文有關通報主管機關之義務，於報告本文分析認為通報主管機關相當重要，而修正條文僅調整為依照主管機關訂定之安維辦法規定有通報義務，但是沒有訂安維辦法的非公務機關就不用通報、或是有訂安維辦法，但是安維辦法沒有通報規定，就不用通報，似乎與報告本文前後不一致，建議再予審視評估。

4. 報告第 311 頁個資法第 27 條之 1 修正條文規定 DPIA 授權由中央目的事業主管機關指定非公務機關執行，但是若沒有指定就不用執行，建議考慮改為不透過指定的方式，明定執行門檻，例如要求達一定筆數、利用敏感個資或蒐集、處理或利用屬「高風險」之行為時，應執行 DPIA(如醫院以 AI 方式進行資料處理及利用)，不論公務或非公務機關均適用，整併至第 18 條修正條文。

5. 報告第 311、312、315 頁個資法第 18 條、第 27 條之 1 修正條文、個資法施行細則第 12 條之 1 修正條文，有關 DPIA 的修正條文提及「評估個人資料之風險」，建議補充說明何謂「風險」。

6. 報告第 316 頁拒絕利用個人資料行銷指引，建議補充說明適用指引的時機與方式，例如：包括合法行銷、違法行銷等。

三、中國文化大學法律學系李教授寧修

(一)建議強化報告第四章修正條文內容與研究結論的關聯性，例如：可針對修正條文增加修正理由。

(二)建議先釐清所欲訂定指引的性質，是供參考之行政指導，抑或具有強制力甚而搭配罰則之適用，如為後者，建議應由法律或法律授權訂定法規命令較為合適。

(三)報告第 307 頁個資法施行細則第 16 條之 1 修正條文，要求控管者向當事人為自動化決策之告知，建議就告知應有相關的配套措施；因為利用開放資料為自動化決策通常是目的外利用之情形，建議將個資法第 9 條之 1 修正條文(目的外利用之告知義務)、第 11 條第 5 項第 6 款(當事人得表達意見)納入施行細則第 16 條之 1 修正條文，以利當事人能知悉並行使其相關權利。

(四)報告第 302 頁的剖析規定的編號遺漏，應該是第 11 款。

(五)報告第 325 頁網路活動資料查詢閱覽權指引中的查詢請求之拒絕，當事人是否有救濟管道？若經公務或非公務機關以指引為依據所為之拒絕，當事人如何救濟？若指引有衍生的法律效果，建議以法律或法律授權訂定法規命令較為適當。

(六)報告第 308 頁個資法第 12 條第 2 項修正條文關於通報主管機關，建議將「行政院及所屬各機關落實個人資料保護聯繫作業要點」相關之重點納入條文，亦可參考資通安全管理法(下稱資安法)之通報義務與程序(例如資安法第 14 條)將公務機關納入規定。報告第 312 頁有關個資法第 48 條修正條文罰則的規定僅針對非公務機關，建議考量是否增加對公務機關的罰則規定，資安法第 19 條規定應有參考價值。

(七)報告第 310 至 315 頁有關個資保護影響評估的修正條文，個資法第 18 條第 4 項及第 5 項、第 27 條之 1 第 2 項及第 3 項、個資法施行細則第 12 條之 1 第 3 項及第 4 項皆為重複內容，建議可予整併。報告第 335 頁個人資料保護影響評估指引，以非公務機關為例，若屬指引要求執行評估，卻未執行者，是否屬於未履行法定義務而將承受不利之法律效果？若將該指引屬行政指導，是否合適？建議釐清。

(八)報告第 267 頁各國 DPIA 規定比較表，參考其他國家大多採法律位階，我國若只以施行細則或指引的方式規範是否適當？建議可再評估。

(九)有關指引的名稱，建議可微調，以資明確，例如：「當事人」拒絕利用個人資料行銷指引、個資侵害事故通知「當事人」指引，僅供參考。

四、研究團隊回應

(一)將於報告中調整日本法的翻譯；以修正對照表的方式補充修法理由。

(二)對於委員所提查閱權、DPIA、自動化決策等建議，將與委託機關討論達成共識後，修改於報告中。

捌、 會議結論：

感謝與會者今日參與並提供寶貴意見，本會將召開工作會議與研究團隊討論後，請研究團隊依委員意見修正期末報告內容並提送本會。

散會（上午 11 時 30 分）

附錄四 期末審查意見回應說明

「強化數位隱私保障所涉個人資料保護法相關議題研析」

委託研究計畫期末審查意見回應說明

委員	編號	建議	研究團隊回應
范姜教授真嫩	1	有關日本文獻翻譯用詞部分： (1) 日文中「者」與「事業」為不同概念，報告第 29 頁「個人資料處理者」與第 93 頁「個人資訊處理事業」，建議統一用詞使用「事業」。 (2) 報告第 29 頁日文條文原文中無「滿足」二字，建議更精確翻譯原文。 (3) 報告第 38 頁引用之日本個人資訊保護法條文應為第30條第5項，建議修正。 (4) 報告第 95 頁「個人關連情報」中「情報」二字為日文用語，建議修正為「個人關連資訊」。	依委員意見調整。
	2	日本行政機關個人資訊保護法的查閱權為避免與政府資訊公開法之規定衝突，故將得拒絕查閱的事由與政府資訊公開法為相	以註腳方式補充可能相當之政府資訊公開法拒絕提供事由之條文，以提醒該指引之使用者。

		同規定。建議可參考日本作法，避免不同法規適用競合產生衝突。	
	3	各國之 DPIA 規定有不同立法政策，且需考量公務或非公務機關的規模、性質、風險、接觸人數等因素，日本尚有「預備評估」、「略式評估」規定，建議做深入分析，釐清立法政策、適用對象、實施方式及利弊得失，再做進一步政策分析。	已依委員意見補充日本個人編號法配套子法關於 DPIA 之規範。
	4	報告第 126 頁標題「目的外利用與利用開放資料為自動化決策之告知」易造成混淆，不清楚是「目的外利用的告知」或是「利用開放資料為自動化決策」，且若以現行目的外利用的合法事由決定是否為目的外利用的告知較不恰當；另外，自動化決策的告知分為兩種，第一為告知當事人會做自動化決策，第二為告知當事人自動化決策的基準、運算邏輯與對其權利之影響，建議分開論述。	(1) 已調整報告第三章第三節標題 (2) 考量目的外利用個資時，當事人個人資料自主權之保障需求，與蒐集時並無實質差異，並為兼顧利用者之利用需求與法遵成本，本研究建議之目的外免告知事由，係以蒐集時免告知事由為基礎，依目的外利用之特性酌作調整。此亦與 GDPR 立法模式一致。 (3) 已補充說明 GDPR 關於告知自動化決策基準、邏輯與影響之規範。
	5	有關個資侵害事故通知當事人，報告第 198 頁建議宜以對當事人權益有「高風險」者作為通知的標	已於報告第三章第四節「修法需求分析」部分補充說明。

		準，請補充關於「高風險」的定義。	
	6	報告第 59 頁拒絕權的公益條款，報告所提依其立法理由似專為新聞業者而生，但是否僅有新聞報導符合公共利益，尚有疑義，建議刪除相關論述，避免爭議。	已刪除新聞業者公益目的相關論述。
劉教授定基	1	報告第 46 頁有關公務機關執行法定職務必要範圍內，因目前法定職務的範圍(包括組織法、法規命令)，相較於歐盟 GDPR 的規定有些不同，或可作為賦予當事人拒絕權的理由。	已補充說明。
	2	報告第 51 頁參考法務部的函釋，論述「當特種個人資料經過提供者處理後已無從識別當事人時，公務機關或學術研究機構取得的資料已非個人資料」，因該函釋尚有爭議，作為賦予學術條款拒絕權的理由較不合適，建議改為參考國外立法例作為理由。	已調整論述。
	3	報告第 85 頁所提由業者自動記錄之數位足跡，是否構成「自消費者取得」的特定個人資訊並適用資訊提供格式要求，似有討論空間等語，建議參考 CCPA 的相關文獻，予以補充。另外建議補充 CCPA 此條規定與第 130 頁所提及 CC	(1) 已補充說明加州就此議題制定施行細則之進展。 (2) 已於第三章第三節加州 CCPA 部分，補充說明自動化決策與查閱權規範之關聯。

		PA 有關自動化決策，二者之關聯性為何？	
	4	報告第 201 頁的結論，對於外洩通知檢討之範圍似乎過窄，建議呈現比較法的差異，例如：「查明後」之文字是否需刪除、是否增加通知期限規定等事項。	已調整個資法通知當事人條文修法草案。
	5	報告第 235 頁關於當事人同意，未納入 GDPR 第 7 條內容的原因為何？若以特定性作為要件，是否包括禁止綑綁同意，似乎不夠明確；參考 GDPR 第 7 條第 2 項規定與其他意思表示應清楚區別之單獨同意，作為同意基本要件，而我國個資法僅有目的外利用有單獨同意的規定，是否需要增訂相關規定，建議於報告中說明，若不增訂，亦請說明不增訂的理由。	已補充於修正條文草案說明欄。
	6	報告第 263、264 頁將 DPIA 的風險分類為因應安全風險與因應當事人權益風險之評估，惟區分標準是否妥適，例如報告將 GDPR 之 DPIA 歸類為因應當事人權益風險之評估，但其似乎亦有包含因應安全風險之評估，建議補充說明分類之理由。	已補充說明兩項分類並非互斥，因應權益風險之評估，內容將涵蓋安全風險評估。

	7	修正條文之體例，建議再為整體評估；體例部分之修正，建議如下： (1) 報告第 303 頁個資法施行細則第 4 條第 7 項修正條文因為與現行個資法施行細則第 3 條都是涉及間接識別個資的定義，建議整併。 (2) 報告第 304 頁個資法第 9 條之 1 修正條文告知義務與現行個資法第 8 條大致相同，建議整併至現有規定。報告第 306 頁個資法施行細則第 16 條第 2 項修正條文僅有在目的外利用才有「不能或需勞費過鉅始能向當事人或其法定代理人為告知」，為何在一般告知無相關規定，建議補充說明理由。 (3) 報告第 309 頁個資法第 14 條之 1 修正條文有關同意的規定，是否需將所有同意條款列出，共通要件或許改為「本法所稱同意」即可。	(1) 細則第 4 條第 7 項係針對「直接或間接識別」個資之例示，並非僅涉間接識別個資，為避免誤會，已調整語句。 (2) 因第 9 條之 1 告知內容係「利用」相關事項，與第 8 條之「蒐集」針對之行為尚有區別，且為強調目的外利用告知義務，本研究認為宜以單獨條文規範。免於告知情形之理由，已補充於修法草案說明欄。 (3) 已調整文句，改為「本法所稱同意」。
	8	修正條文草案及指引實質內容之修正建議如下： (1) 第 299 頁個資法第 11 條第 5 項第 2 款修正條文「且資料未經提供者處理至無從識別特定之當事人」，現行法的問題對於「無從識別特定當事人」之定義尚有爭	(1) 已調整為蒐集機關以其所保有之資料，得以識別特定當事人時，方得對研究所涉個資蒐集處理利用使拒絕權。 (2) 自動化決策效果之告知，見於細則修正條文第 16 條之 1

		議，建議參考報告中對於查閱權之研究，於蒐集機關無對照組合資料得識別當事人之情形，蒐集機關並無義務為滿足當事人之請求而使用額外資訊為識別特定個人。 (2) 報告第 307 頁個資法施行細則第 16 條之 1 修正條文「向當事人告知該個人資料之蒐集目的與利用方式」，已經是現行個資法第 8 條規定之範圍，修正條文用語無法呈現額外應告知之事項，建議增加告知自動化決策涉及的邏輯與效果。 (3) 報告第 308 頁個資法第 12 條修正條文有關通報主管機關之義務，於報告本文分析認為通報主管機關相當重要，而修正條文僅調整為依照主管機關訂定之安維辦法規定有通報義務，但是沒有訂安維辦法的非公務機關就不用通報、或是有訂安維辦法，但是安維辦法沒有通報規定，就不用通報，似乎與報告本文前後不一致，建議再予審視評估。 (4) 報告第 311 頁個資法第 27 條之 1 修正條文規定 DPIA 授權由中央目的	第 2 項，已調整文句，以資明確。 (3) 併陳兩案修正條文供委託機關參考。 (4) 已調整為以「高風險」為標準執行 DPIA 標準，不需主管機關指定，且其執行方式準用第 18 條非公務機關相關規定。惟個資處理筆數門檻部分，似不宜於個資法中直接明定，待日後成立專責機關後，由專責機關確定。 (5) 已調整為「蒐集、處理或利用對當事人隱私及其他權益」。 (6) 已補充說明。

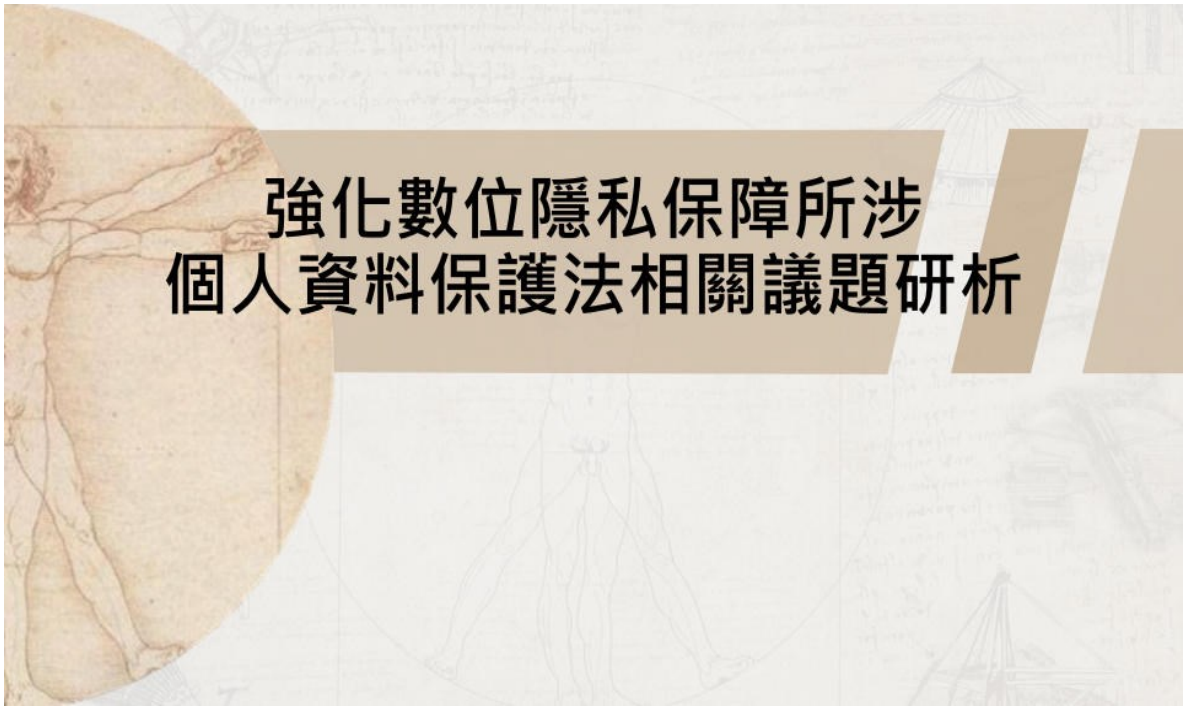
		事業主管機關指定非公務機關執行，但是若沒有指定就不用執行，建議考慮改為不透過指定的方式，明定執行門檻，例如要求達一定筆數、利用敏感個資或蒐集、處理或利用屬「高風險」之行為時，應執行DPIA(如醫院以AI方式進行資料處理及利用)，不論公務或非公務機關均適用，整併至第18條修正條文。 (5) 報告第 311、312、315 頁個資法第18條、第27條之1修正條文、個資法施行細則第 12 條之1修正條文，有關 DPIA 的修正條文提及「評估個人資料之風險」，建議補充說明何謂「風險」。 (6) 報告第 316 頁拒絕利用個人資料行銷指引，建議補充說明適用指引的時機與方式，例如：包括合法行銷、違法行銷等。	
李教授寧修	1	建議強化報告第四章修正條文內容與研究結論的關聯性，例如：可針對修正條文增加修正理由。	已補充修正條文說明欄。
	2	建議先釐清所欲訂定指引的性質，是供參考之行政指導，抑或具有強制力甚而搭配罰則之適用，如為後者，建議應由法律或法	已於報告本文及附件各指引補充說明指引皆不具法律拘束力。

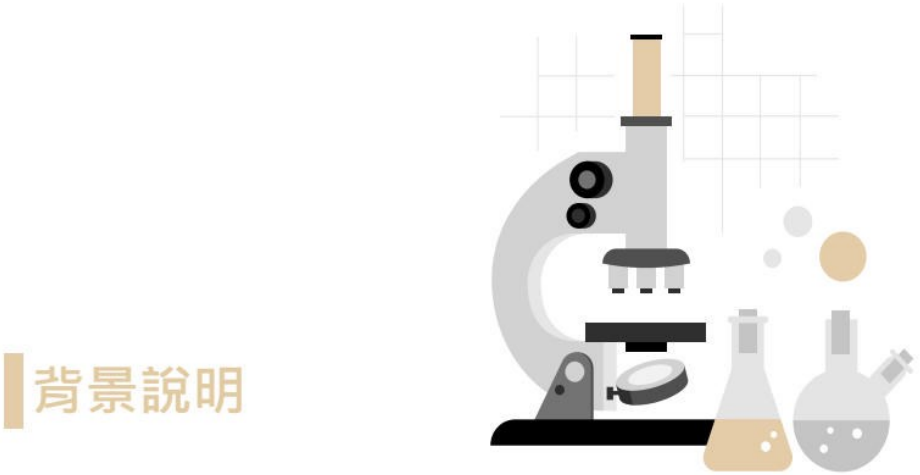
		律授權訂定法規命令較為合適。	
	3	報告第307頁個資法施行細則第16條之1修正條文，要求控管者向當事人為自動化決策之告知，建議就告知應有相關的配套措施；因為利用開放資料為自動化決策通常是目的外利用之情形，建議將個資法第9條之1修正條文(目的外利用之告知義務)、第11條第5項第6款(當事人得表達意見)納入施行細則第16條之1修正條文，以利當事人能知悉並行使其相關權利。	考量施行細則增訂自動化決策告知與個資法增訂目的外利用告知時序尚難確定，將細則修正條文調整為「依本法關於告知當事人之規定」向當事人告知自動化決策事項，以保留彈性。
	4	報告第302頁的剖析規定的編號遺漏，應該是第11款。	已補充編號。
	5	報告第325頁網路活動資料查詢閱覽權指引中的查詢請求之拒絕，當事人是否有救濟管道？若經公務或非公務機關以指引為依據所為之拒絕，當事人如何救濟？若指引有衍生的法律效果，建議以法律或法律授權訂定法規命令較為適當。	(1) 非公務機關如拒絕查閱網路活動資料，應循查閱請求救濟之一般管道。公務機關如拒絕查閱，當事人得依相關法律提起訴願或訴訟（個資法第13條立法理由參照）。 (2) 本研究所提指引草案目的係依個資法提示優良實務，並無法律拘束力，司法機關等於審查救

			濟請求時，得本於權責判斷拒絕查閱是否合於個資法。
	6	報告第 308 頁個資法第 12 條第 2 項修正條文關於通報主管機關，建議將「行政院及所屬各機關落實個人資料保護聯繫作業要點」相關之重點納入條文，亦可參考資通安全管理法(下稱資安法)之通報義務與程序(例如資安法第 14 條)將公務機關納入規定。報告第 312 頁有關個資法第 48 條修正條文罰則的規定僅針對非公務機關，建議考量是否增加對公務機關的罰則規定，資安法第 19 條規定應有參考價值。	(1) 條文已調整。 (2) 現行規定下，公務機關(及其人員)如違反個資法，應回歸公務員服務法、懲戒法、考績法等規範。至於資安法第 19 條授權主管機關（行政院）訂定公務機關所述人員違反該法之懲處辦法，似宜待個資法設立獨立專責機關後再研議。
	7	報告第 310 至 315 頁有關個資保護影響評估的修正條文，個資法第 18 條第 4 項及第 5 項、第 27 條之 1 第 2 項及第 3 項、個資法施行細則第 12 條之 1 第 3 項及第 4 項皆為重複內容，建議可予整併。報告第 335 頁個人資料保護影響評估指引，以非公務機關為例，若屬指引要求執行評估，卻未執行者，是否屬於未履行法定義務而將承受不利之法律效果？若將該指引屬行政指導，是否合適？建議釐清。	(1) 個資法修正條文已調整為第 27 條準用第 18 條。因施行細則修正條文非以修法為前提，故仍保留相關內容，但增加相關說明，以免誤會。 (2) 本研究目前提出之個人資料保護影響評估指引係搭配施行細則修正條文，向「依細則應執行評估」之機關提示優良實務做法。何者有義務執行評估，係依施行細則確定，故應不生「指引要求執行評

			估，卻未執行」之問題。
	8	報告第 267 頁各國 DPIA 規定比較表，參考其他國家大多採法律位階，我國若只以施行細則或指引的方式規範是否適當？建議可再評估。	本研究認同若以法律位階規定 DPIA，將更利於強化當事人資訊隱私權保障，故提供「修正個資法」方案。惟考量 DPIA 所涉法遵成本及對我國社會行業之衝擊，本研究亦同時提供「修正施行細則並搭配指引」方案，供主管機關參考。
	9	有關指引的名稱，建議可微調，以資明確，例如：「當事人」拒絕利用個人資料行銷指引、個資侵害事故通知「當事人」指引，僅供參考。	已依建議調整。

附錄五 研究成果簡報





本案需求

研究議題(歐、美、日、韓、新、我國)		
當事人拒絕權	查閱權（查閱標的）	個資外洩通知
目的外利用 / 自動化決策告知義務		當事人同意
個資衝擊影響評估		個資保護官(長)

配合事項
開放政府行動方案焦點座談會：110.05.06(1)、08.05(2)

期中產出
7項議題的修法需求，或以指引補充即可

期末產出
修法條文草案、指引草案

人力配置與任務分工

專案執行進度規劃

工作項目	第1個月	第2個月	第3個月	第4個月	第5個月	第6個月	第7個月
當事人拒絕權							
當事人查詢或閱覽權							
告知義務 (目的外利用)							
個資外洩通知							
當事人同意							
個資衝擊 影響評估							
個資保護官(DPO)							
修法建議							
指引草案							
審查會議							

▲ 交付工作計畫書，▲ 交付期中報告(各議題是否發布指引或修法建議)，▲ 交付期末報告(指引草案內容或修法條文之具體建議)，

修法條文與指引草案

修法條文

指引草案

修正個資法條文，增訂當事人對合法蒐集、處理、利用個資之行為行使拒絕權之原則與例外。

修正條文	現行條文
第十一條 I. 公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。II. 個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議者，不在此限。 III. 個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。 IV. 違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。	第十一條 I. 公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。 II. 個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議者，不在此限。 III. 個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。 IV. 違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。

修法條文

指引草案

修正條文	現行條文
第十一條 V. 有下列情形之一者，公務機關或非公務機關雖未違反本法規定蒐集、處理或利用個人資料，仍應依當事人之請求，停止蒐集、處理或利用其個人資料： 一、依第六條第一項但書第三款或第十九條第一項第三款規定，蒐集、處理或利用個人資料。 二、依第六條第一項但書第四款、第十六條但書第五款、第十九條第一項第四款或第二十條第一項但書第五款規定，蒐集、處理或利用個人資料，且蒐集者以其所保有之資訊，得以該資料識別特定之當事人。 三、依第十六條但書第二款後段、第十九條第一項第六款或第二十條第一項但書第二款規定，蒐集、處理或利用個人資料。但能證明所追求之公共利益顯優於當事人之權益者，不在此限。 四、依第十五條第三款或第十九條第一項第八款規定，蒐集、處理個人資料。 五、依第十六條但書第六款或第二十條第一項但書第七款規定，利用個人資料。 VI. 公務機關或非公務機關僅以自動化決策對當事人作成具有法律效果或類似重大效果之決定者，當事人有權拒絕而不受該決定之拘束。但有下列情形之一，且蒐集機關已提供當事人請求人為介入自動化決策，並對自動化決策陳述意見之機會者，不在此限： 一、自動化決策為締結或履行蒐集機關與當事人間之契約或類似契約所必要。 二、經當事人同意。 VII. 因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。	第十一條 V. 因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。

修法條文

修正條文	現行條文
第十一條 V. 有下列情形之一者，公務機關或非公務機關雖未違反本法規定蒐集、處理或利用個人資料，仍應依當事人之請求，停止蒐集、處理或利用其個人資料： 一、依第六條第一項但書第三款或第十九條第一項第三款規定，蒐集、處理或利用個人資料。 二、依第六條第一項但書第四款、第十六條但書第五款、第十九條第一項第四款或第二十條第一項但書第五款規定，蒐集、處理或利用個人資料，且蒐集者以其所保有之資訊，得以該資料識別特定之當事人。 三、依第十六條但書第二款後段、第十九條第一項第六款或第二十條第一項但書第二款規定，蒐集、處理或利用個人資料。但能證明所追求之公共利益顯優於當事人之權益者，不在此限。 四、依第十五條第三款或第十九條第一項第八款規定，蒐集、處理個人資料。 五、依第十六條但書第六款或第二十條第一項但書第七款規定，利用個人資料。 VI. 公務機關或非公務機關僅以自動化決策對當事人作成具有法律效果或類似重大效果之決定者，當事人有權拒絕而不受該決定之拘束。但有下列情形之一，且蒐集機關已提供當事人請求人為介入自動化決策，並對自動化決策陳述意見之機會者，不在此限： 一、自動化決策為締結或履行蒐集機關與當事人間之契約或類似契約所必要。 二、經當事人同意。 VII. 因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。	第十一條 V. 因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。

指引草案

拒絕權 查閱權 告知範圍 個資外洩通知 當事人同意 個資衝擊影響評估 個資保護官

修法條文

指引草案

針對拒絕行銷訂定指引草案。

首次利用個人資料行銷時：

非公務機關應向當事人告知得拒絕接受行銷，亦應提供當事人表示拒絕接受行銷之方式，並支付所需費用：

- 通話方式：明確向當事人告知拒絕權；
- 簡訊方式：提供行使拒絕權電話/簡訊的電話號碼；
- Email方式：勾選取消等方式；
- 紙本方式：提供表格&回郵信封。

當事人表示拒絕接受行銷時：

- 當事人對行銷得任意拒絕。
- 以同意為依據蒐集處理利用，當事人撤回同意即同於拒絕接受行銷。
- 當事人表達拒絕接受行銷之意時，非公務機關即應停止利用其個人資料行銷，其後亦不得再利用其個人資料行銷。
- 當事人行使拒絕權之方式，不以非公務機關提供之方式為限。

當事人表示拒絕接受行銷後：

- 非公務機關應以適當方式保存並及時更新拒絕接受行銷之當事人名單。
- 非公務機關應採取措施確保行銷業務人員取得當下正確之未拒絕接受行銷當事人名單。
- 非公務機關如設營業據點或分公司，應採取措施收集、統整並傳達拒絕接受行銷當事人名單。
- 當事人表達拒絕行銷後，即應檢視是否需要刪除、停止處理或利用特定目的已消失之個人資料。

其他事項：

- 非公務機關委託他人利用個人資料向當事人行銷，應採取適當之監督措施。
- 於委託他人行銷之情形，當事人應有權選擇向受託者或委託之非公務機關表示拒絕接受行銷。
- 數非公務機關共同向當事人行銷之情形，當事人向任一方表示拒絕接受行銷之意思時，除當事人有相反表示，應視為當事人拒絕接受所有非公務機關利用其個人資料行銷。

達文西個資暨高科技法律事務所 /強化數位隱私保障所涉個人資料保護法相關議題研析

拒絕權 | 查閱權 | 告知範圍 | 個資外洩通知 | 當事人同意 | 個資衝擊影響評估 | 個資保護官

修法條文

指引草案

修正個資法施行細則，增訂數位足跡為個人資料之例示。

修正條文	現行條文
第四條 I. 本法第二條第一款所稱病歷之個人資料，指醫療法第六十七條第二項所列之各款資料。 II. 本法第二條第一款所稱醫療之個人資料，指病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方、用藥、施術或處置所產生之個人資料。 III. 本法第二條第一款所稱基因之個人資料，指由人體一段去氧核醣核酸構成，為人體控制特定功能之遺傳單位訊息。 IV. 本法第二條第一款所稱性生活之個人資料，指性取向或性慣行之個人資料。 V. 本法第二條第一款所稱健康檢查之個人資料，指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料。 VI. 本法第二條第一款所稱犯罪前科之個人資料，指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄。 VII. 本法第二條第一款所稱個人資料，包括因使用網路產品或服務所產生，或與該使用相關，且得以直接或間接識別該個人之資料，如網路識別碼、網路活動紀錄及基於網路活動而推知之資料。	第四條 I. 本法第二條第一款所稱病歷之個人資料，指醫療法第六十七條第二項所列之各款資料。 II. 本法第二條第一款所稱醫療之個人資料，指病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方、用藥、施術或處置所產生之個人資料。 III. 本法第二條第一款所稱基因之個人資料，指由人體一段去氧核醣核酸構成，為人體控制特定功能之遺傳單位訊息。 IV. 本法第二條第一款所稱性生活之個人資料，指性取向或性慣行之個人資料。 V. 本法第二條第一款所稱健康檢查之個人資料，指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料。 VI. 本法第二條第一款所稱犯罪前科之個人資料，指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄。

拒絕權 | 查閱權 | 告知範圍 | 個資外洩通知 | 當事人同意 | 個資衝擊影響評估 | 個資保護官

修法條文

指引草案

就數位足跡如何行使查閱權及其範圍訂定指引草案。

網路活動資料之含義&管理：

- 網路識別碼，包含IP位址、Mac位址、cookie或類似追蹤識別碼、使用者裝置識別碼、使用者帳號及名稱等。
- 網路活動紀錄，包含登入、搜尋、點選、瀏覽、輸入、同步、匯出、刪除等網路活動之紀錄。
- 基於網路活動而推知之資料，包含對該個人偏好、興趣、經濟狀況、行為、健康、位置、能力等特徵之分析、評估或預測。
- 公務機關或非公務機關宜根據網路活動資料之特徵，就網路活動資料之蒐集、處理及利用訂定適當管理程序。

網路活動資料查閱請求之提出&確認：

- 公務機關或非公務機關宜向當事人提供提出網路活動資料查閱請求之便利管道，告知請求回應時程、收費標準及其他應釋明之事項，並保留所受理請求之紀錄。
- 當事人網路活動資料查閱請求表明查閱網路活動資料之意願即足，不以使用法律術語或援引本法條文為必要。
- 公務機關或非公務機關應建立適當程序，及時合理確認提出網路活動資料查閱請求之當事人身分，不得無故遲延。
- 公務機關或非公務機關提供帳號密碼登入驗證程序者，當事人依其程序登入帳號，應視為已確認身分，但公務機關或非公務機關有合理認為需進一步確認者，不在此限。

網路活動資料查閱請求之審查回覆：

- 公務機關或非公務機關應建立適當程序，完整搜尋與彙整網路活動資料查閱請求所涉資料。
- 以現有資料不能識別當事人者，公務機關或非公務機關無須為回應當事人請求之唯一目的，蒐集、處理或利用該當事人之其他資料，但當事人為行使權利目的提供其他資料以實現識別者，不在此限。
- 公務機關或非公務機關宜以當事人提出請求之相同方式回覆該請求，但當事人另有要求、或當事人提出請求之方式不適於回覆者，不在此限。
- 公務機關或非公務機關拒絕當事人網路活動資料查閱請求者，以請求所涉資料中存在事實上不能或本法第10條但書所列例外情事者為限，且應將拒絕原因以書面通知當事人。

達文西個資暨高科技法律事務所 /強化數位隱私保障所涉個人資料保護法相關議題研析

修法條文

指引草案

修正個資法，參考個資法第8條與第9條的蒐集告知例外條款之立法方式，納入目的外利用的告知原則與例外。

修正條文	現行條文
第七條 I. 第十五條第二款及第十九條第一項第五款所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。 II. 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第九條之一第一項各款應告知事項及同意與否對其權益之影響後，單獨所為之意思表示。 III. 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。 IV. 蒐集者就本法所稱經當事人同意之事實，應負舉證責任。	第七條 I. 第十五條第二款及第十九條第一項第五款所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。 II. 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。 III. 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。 IV. 蒐集者就本法所稱經當事人同意之事實，應負舉證責任。

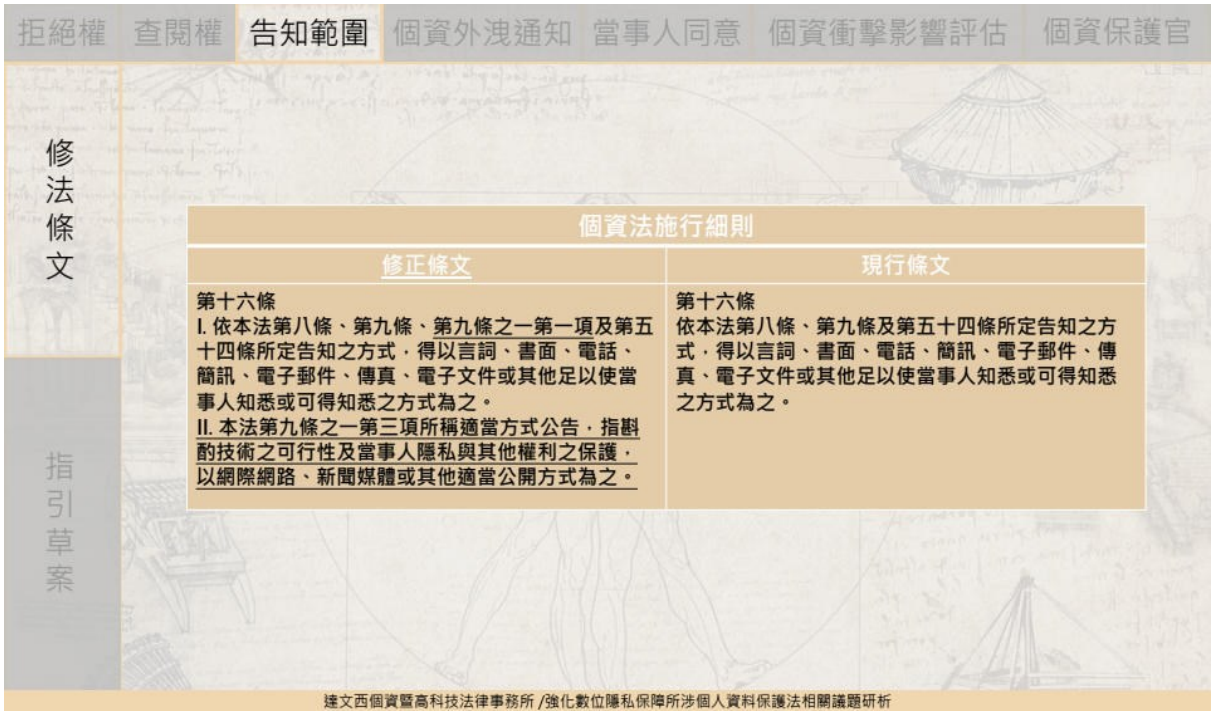
拒絕權 查閱權 告知範圍 個資外洩通知 當事人同意 個資衝擊影響評估 個資保護官

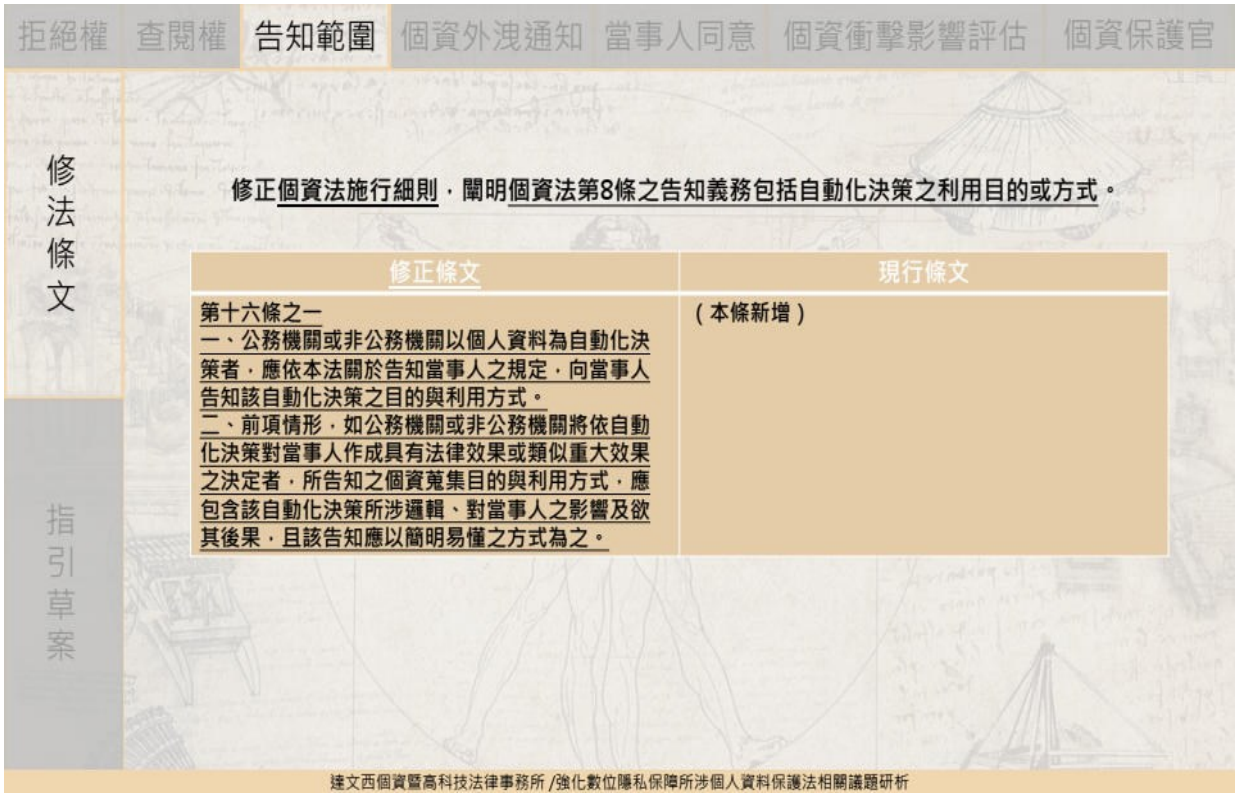
修法條文

指引草案

修正條文	現行條文
第九條之一 I. 公務機關或非公務機關依第十六條但書或第二十條第一項但書規定利用個人資料時，應於利用前明確向當事人告知下列事項： 一、公務機關或非公務機關名稱。 二、利用之目的。 三、利用之個人資料或其類別。 四、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。 II. 有下列情形之一者，得免為前項之告知： 一、依法律規定得免告知。 二、個人資料之利用係公務機關執行法定職務或非公務機關履行法定義務所必要。 三、告知將使公務機關或非公務機關違反法律規定之保密義務。 四、當事人明知應告知之內容。 五、不能或需勞費過鉅始能向當事人或其法定代理人為告知。 六、告知將損害當事人或他人之生命、身體或財產利益，或有損害之虞。 七、告知將嚴重損害利用機關之權利或正當利益。 III. 前項第五款情形，利用機關應將第一項各款事項以適當方式公告。 第七條 I. 第十五條第二款及第十九條第一項第五款所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。 II. 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第九條之一第一項各款應告知事項及同意與否對其權益之影響後，單獨所為之意思表示。 III. 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。 IV. 蒐集者就本法所稱經當事人同意之事實，應負舉證責任。	(本條新增)

達文西個資暨高科技法律事務所 /強化數位隱私保障所涉個人資料保護法相關議題研析


拒絕權
查閱權
告知範圍
個資外洩通知
當事人同意
個資衝擊影響評估
個資保護官
修法條文
指引草案
個資法施行細則
修正條文
現行條文
第十六條
I. 依本法第八條、第九條、第九條之一第一項及第五十四條所定告知之方式，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。
II. 本法第九條之一第三項所稱適當方式公告，指斟酌技術之可行性及當事人隱私與其他權利之保護，以網際網路、新聞媒體或其他適當公開方式為之。
第十六條
依本法第八條、第九條及第五十四條所定告知之方式，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。
達文西個資暨高科技法律事務所 /強化數位隱私保障所涉個人資料保護法相關議題研析


拒絕權
查閱權
告知範圍
個資外洩通知
當事人同意
個資衝擊影響評估
個資保護官
修法條文
指引草案
修正個資法施行細則，闡明個資法第8條之告知義務包括自動化決策之利用目的或方式。
修正條文
現行條文
第十六條之一
一、公務機關或非公務機關以個人資料為自動化決策者，應依本法關於告知當事人之規定，向當事人告知該自動化決策之目的與利用方式。
二、前項情形，如公務機關或非公務機關將依自動化決策對當事人作成具有法律效果或類似重大效果之決定者，所告知之個資蒐集目的與利用方式，應包含該自動化決策所涉邏輯、對當事人之影響及欲其後果，且該告知應以簡明易懂之方式為之。
（本條新增）
達文西個資暨高科技法律事務所 /強化數位隱私保障所涉個人資料保護法相關議題研析

修法條文

指引草案

修正個資法，增訂將個資侵害事故通報主管機關之要求，並調整現行個資侵害事故通知當事人之判定標準，引入當事人權益風險之考量要素。

修正條文	現行條文
第十二條 公務機關或非公務機關發生個人資料被竊取、洩漏、竄改或其他侵害，可能導致當事人隱私或其他權利保護高風險者，應以適當方式通知當事人，不得無故遲延。	第十二條 公務機關或非公務機關違反本法規定，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。
第十二條之一 （甲案） 非公務機關發生個人資料被竊取、洩漏、竄改或其他侵害者，應依中央目的事業主管機關依第二十七條第二項、第三項授權訂定之辦法通報。 （乙案） 非公務機關發生個人資料被竊取、洩漏、竄改或其他侵害者，應立即通報中央目的事業主管機關或直轄市、縣（市）政府，至遲於知悉該侵害事故後七十二小時內為之。但中央目的事業主管機關依第二十七條第二項、第三項授權訂定之辦法就通報對象、方式等事項方式另有規定者，從其規定。 前項通報對象有疑義者，非公務機關得通報各有權管轄之中央目的事業主管機關與直轄市、縣（市）政府。	（本條新增）

修法條文

指引草案

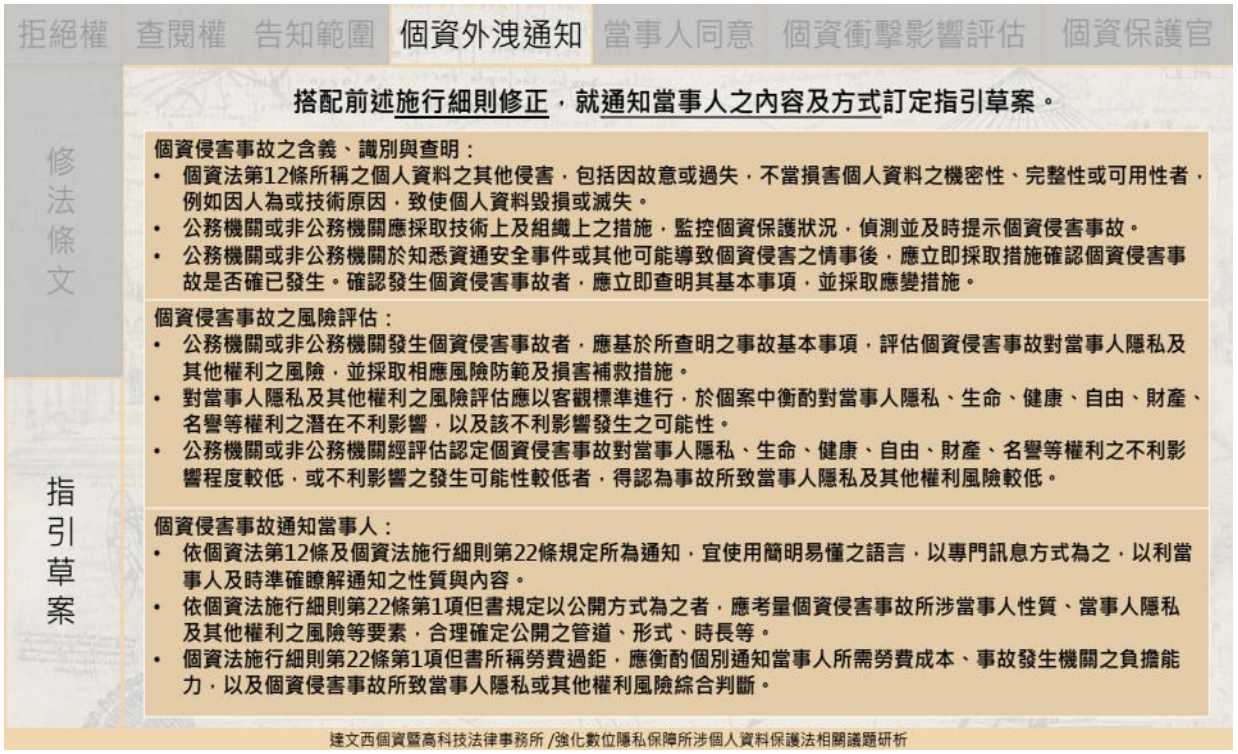
修正條文	現行條文
第四十八條 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰： 一、違反第八條或第九條規定。 二、違反第十條、第十一條、第十二條、第十二條之一或第十三條規定。 三、違反第二十條第二項或第三項規定。 違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。	第四十八條 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰： 一、違反第八條或第九條規定。 二、違反第十條、第十一條、第十二條或第十三條規定。 三、違反第二十條第二項或第三項規定。 違反第二十七條第一項或未依第二項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。

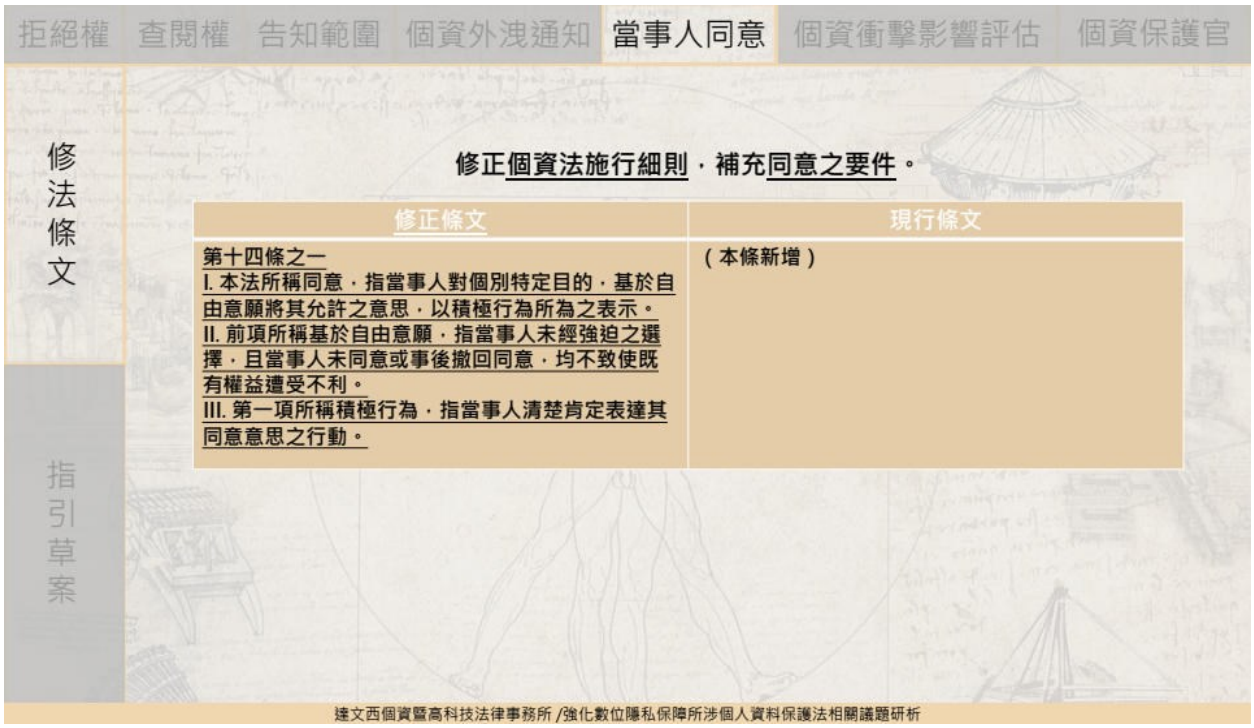
修法條文

指引草案

修正個資法施行細則第22條，以其他用語取代「需費過鉅」。

修正條文	現行條文
第二十二條 I. 本法第十二條所稱適當方式通知當事人，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但通知所需勞費過鉅者，得斟酌技術之可行性及當事人隱私與其他權利之保護，以網際網路、新聞媒體或其他適當公開方式為之。 II. 依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。	第二十二條 I. 本法第十二條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。 II. 依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。


拒絕權
查閱權
告知範圍
個資外洩通知
當事人同意
個資衝擊影響評估
個資保護官
修法條文
指引草案
搭配前述施行細則修正，就通知當事人之內容及方式訂定指引草案。
個資侵害事故之含義、識別與查明：
• 個資法第12條所稱之個人資料之其他侵害，包括因故意或過失，不當損害個人資料之機密性、完整性或可用性者，例如因人為或技術原因，致使個人資料毀損或滅失。
• 公務機關或非公務機關應採取技術上及組織上之措施，監控個資保護狀況，偵測並及時提示個資侵害事故。
• 公務機關或非公務機關於知悉資通安全事件或其他可能導致個資侵害之情事後，應立即採取措施確認個資侵害事故是否確已發生。確認發生個資侵害事故者，應立即查明其基本事項，並採取應變措施。
個資侵害事故之風險評估：
• 公務機關或非公務機關發生個資侵害事故者，應基於所查明之事故基本事項，評估個資侵害事故對當事人隱私及其他權利之風險，並採取相應風險防範及損害補救措施。
• 對當事人隱私及其他權利之風險評估應以客觀標準進行，於個案中衡酌對當事人隱私、生命、健康、自由、財產、名譽等權利之潛在不利影響，以及該不利影響發生之可能性。
• 公務機關或非公務機關經評估認定個資侵害事故對當事人隱私、生命、健康、自由、財產、名譽等權利之不利影響程度較低，或不利影響之發生可能性較低者，得認為事故所致當事人隱私及其他權利風險較低。
個資侵害事故通知當事人：
• 依個資法第12條及個資法施行細則第22條規定所為通知，宜使用簡明易懂之語言，以專門訊息方式為之，以利當事人及時準確瞭解通知之性質與內容。
• 依個資法施行細則第22條第1項但書規定以公開方式為之者，應考量個資侵害事故所涉當事人性質、當事人隱私及其他權利之風險等要素，合理確定公開之管道、形式、時長等。
• 個資法施行細則第22條第1項但書所稱勞費過鉅，應衡酌個別通知當事人所需勞費成本、事故發生機關之負擔能力，以及個資侵害事故所致當事人隱私或其他權利風險綜合判斷。
達文西個資暨高科技法律事務所 /強化數位隱私保障所涉個人資料保護法相關議題研析


拒絕權
查閱權
告知範圍
個資外洩通知
當事人同意
個資衝擊影響評估
個資保護官
修法條文
指引草案
修正個資法施行細則，補充同意之要件。
修正條文
現行條文
第十四條之一
I. 本法所稱同意，指當事人對個別特定目的，基於自由意願將其允許之意思，以積極行為所為之表示。
II. 前項所稱基於自由意願，指當事人未經強迫之選擇，且當事人未同意或事後撤回同意，均不致使既有權益遭受不利。
III. 第一項所稱積極行為，指當事人清楚肯定表達其同意意思之行動。
（本條新增）
達文西個資暨高科技法律事務所 /強化數位隱私保障所涉個人資料保護法相關議題研析

修法條文

指引草案

修正個資法，增訂強制執行個資保護影響評估之情形。

修正條文	現行條文
第十八條 I. 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。 II. 公務機關蒐集、處理或利用個人資料之行為，或該行為涉及之系統，依其性質、背景、目的與範圍，對當事人權益有高風險之虞者，應於行為前或系統使用前，執行個人資料保護影響評估。 III. 有下列情形之一者，視為前項所稱對當事人權益有高風險之虞： 一、對當事人為評估或評分（包含剖析）。 二、具有法律效果或類似重大效果之自動化決策。 三、對當事人之系統性監控。 四、涉及本法第六條之個人資料。 五、依涉及人數、資料數量、持續時間等條件，大規模蒐集、處理或利用個人資料。 六、匹配或組合不同資料集。 七、蒐集、處理或利用弱勢當事人之個人資料。 八、創新利用或應用新的技術性或組織性解決方案。 九、該行為之將阻止當事人行使權利、使用服務或締結契約。	第十八條 I. 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。

拒絕權 查閱權 告知範圍 個資外洩通知 當事人同意 個資衝擊影響評估 個資保護官

修法條文

指引草案

修正條文	現行條文
IV. 第二項所稱個人資料保護影響評估，至少應包括下列事項： 一、識別集、處理或利用個人資料之行為、範圍與流程。 二、檢視蒐集、處理或利用個人資料之合目的性與合比例性。 三、評估個人資料蒐集、處理或利用行為對當事人隱私及其他權益之風險。 四、規劃風險因應措施。 V. 公務機關應依個人資料保護影響評估結果，採取規劃之風險因應措施以避免或降低風險，並應持續監控剩餘風險，即時改善風險因應措施之有效性。	

達文西個資暨高科技法律事務所 /強化數位隱私保障所涉個人資料保護法相關議題研析

修法條文

指引草案

修正條文	現行條文
IV. 第二項所稱個人資料保護影響評估，至少應包括下列事項： 一、識別蒐集、處理或利用個人資料之行為、範圍與流程。 二、檢視蒐集、處理或利用個人資料之合目的性與合比例性。 三、評估個人資料蒐集、處理或利用行為對當事人隱私及其他權益之風險。 四、規劃風險因應措施。 V. 公務機關應依個人資料保護影響評估結果，採取規劃之風險因應措施以避免或降低風險，並應持續監控剩餘風險，即時改善風險因應措施之有效性。	

修法條文

指引草案

如暫不於個資法中增訂強制執行個資保護影響評估之規範，可修正個資法施行細則，細部說明個資保護影響評估之適用情況、範圍、項目。

修正條文	現行條文
第十二條之一 I公務機關或非公務機關蒐集、處理或利用個人資料之行為，或該行為涉及之系統，依其性質、背景、目的與範圍，對當事人權益有高風險之虞者，前條第2項第3款之個人資料之風險評估，得包含個人資料保護影響評估，並於行為前或系統使用前為之。 II前項所稱對當事人權益有高風險之虞，包含但不限於下列各款情形之一： 一、對當事人為評估或評分（包含剖析） 二、具有法律效果或類似重大效果之自動化決策。 三、對當事人之系統性監控。 四、涉及本法第六條之個人資料。 五、依涉及人數、資料數量、持續時間等條件，大規模蒐集、處理或利用個人資料。 六、匹配或組合不同資料集。 七、蒐集、處理或利用弱勢當事人之個人資料。 八、創新利用或應用新的技術性或組織性解決方案。 九、該行為之將阻止當事人行使權利、使用服務或締結契約。 III第一項所稱個人資料保護影響評估，至少應包括下列事項： 一、識別蒐集、處理或利用個人資料之行為、範圍與流程。 二、檢視蒐集、處理或利用個人資料之合目的性與合比例性。 三、評估個人資料之風險。 四、規劃風險因應措施。 IV公務機關或非公務機關應依個人資料保護影響評估結果，採取規劃之風險因應措施以避免或降低風險，並應持續監控剩餘風險，即時改善風險因應措施之有效性。	（本條新增）

修法條文

指引草案

依前述修正之施行細則訂定指引草案。

個資保護影響評估之步驟：

- 識別蒐集、處理或利用個人資料之行為、範圍與流程：
  - 個人資料蒐集、處理或利用行為之背景、目的、所涉資源，以及所涉個人資料之內容、保存方式與期限；
  - 將個人資料提供予第三人（包含受機關委託之受託者）者，該第三人或其業別。
- 檢視蒐集、處理或利用個人資料之合目的性與合比例性：
  - 該行為之目的應特定、明確、合法；
  - 該行為僅蒐集、處理或利用適當、相關且必要之個人資料。
- 評估個人資料保護法之遵循性：
  - 蒐集、處理與利用個人資料之法律依據，以同意為依據者；同意之合法性，告知義務之存否與踐行方式；
  - 評估個人資料之正確性維持與保存期限，當事人權利之行使，個資境外傳輸限制，個資侵害事故通知機制；
  - 委託他人蒐集、處理或利用個人資料者，對受託者之監督。
- 鑑別個人資料之風險：
  - 以當事人權益受影響程度，鑑別風險種類與來源，並宜徵詢機關內外關係人之意見；
  - 鑑別風險發生之可能性，以及風險發生對當事人權益影響之嚴重性。
- 依據鑑別之風險，預先規劃足以避免或降低風險之因應措施。

個資保護影響評估之結果：

- 機關應將個資保護影響評估結果與決策作成紀錄。
- 機關應依個資保護影響評估結果，對該行為或涉及之系統，採取規劃之風險因應措施。
- 機關應持續監控剩餘風險，即時改善風險因應措施之有效性

修法條文

指引草案

個資保護官（DPO）制度比較研究發現

DPO制度之目標：

- 負責個資安全維護之個資保護官：
  - DPO之核心職責係採行安全維護措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
  - 我國個資法之指定專人負責制度即屬此類。
- 負責執行個資法遵之個資保護官：
  - DPO之核心職責，係實際執行個資法規之 各項要求，確保個人資料蒐集處理利用機關遵守個資法規。
  - 韓國個人情報保護法之個人資料保護責任者和新加坡 PDPA 所規定之 DPO 皆屬此類。
- 負責個資安全維護之個資保護官：
  - DPO之核心職責，係協助個人資料蒐集處 理利用機關遵守個資法規，並承擔諮詢與監督職能。
  - 歐盟 GDPR 所規定之 DPO 制度即屬此類。

指派DPO之義務：

- 負責個資安全維護之個資保護官：
  - 我國：須注重個人資料安全之機關，例如公務機關，以及目的事業主管機關指定之非公務機關，強制指派專人負責個資安全維護事項。
- 負責執行個資法遵之個資保護官：
  - 韓國：所有個人資料處理者皆須指派個人資料保護責任者，且非公務機關之個人資料保護責任者通常由業主擔任。
  - 新加坡：各組織皆應指派一名或多名DPO。
- 負責個資安全維護之個資保護官：
  - 歐盟： 公務機關，或控管者或處理者之核心業務所涉個資處理作業，需大規模經常性且系統性監控當事人、大規模處理特種個資或前科或 犯罪個資之高風險情形，強制指派 DPO。

結論

議題修訂彙整表

	拒絕權	查閱權	告知範圍	個資外洩通知	當事人同意	個資衝擊影響評估	個資保護官
修正個資法	√		√	√		√	
修正個資法施行細則		√	√	√	√	√	
訂定指引草案	√	√		√		√	
暫不提出相關修正							√

謝謝聆聽

THANKS FOR YOUR ATTENTION

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

強化數位隱私保障所涉個人資料保護法相關議題研析/葉奇鑫計畫主持 -- 初版. -- 臺北市 : 國發會, 民 110.11

面: 表，公分

編號: (110)011.0904

委託單位：國家發展委員會

受託單位：達文西個資暨高科技法律事務所

資訊隱私權
580

強化數位隱私保障所涉個人資料保護法相關議題研析
委託單位：國家發展委員會
受託單位：達文西個資暨高科技法律事務所
計畫主持人：葉奇鑫
出版機關：國家發展委員會
電話：02-23165300
地址：臺北市寶慶路 3 號
網址：http://www.ndc.gov.tw/
出版年月：中華民國 110 年 11 月
版次：初版
刷次：第 1 刷
編號：(110) 011.0904 (平裝)