行政院所屬各機關因公出國報告書

(出國類別：考察)

考察南韓個人資料保護獨立機關制度與實務運作出國報告

出國人員服務機關	職　稱	姓　名
個人資料保護委員會籌備處	組　長	張育綾
個人資料保護委員會籌備處	組　長	林逸塵
個人資料保護委員會籌備處	視　察	陳樂庭
財團法人資訊工業策進會	資深研究協理	邱映曦
南臺科技大學	副教授	郭戎晉

考察國家：南韓

出國期間：民國 113 年 7 月 23 日至 113 年 7 月 26 日

報告日期：民國 113 年 10 月

摘要

本次考察主要針對南韓個人資料保護委員會及與其執法、立法相關之代表性單位或組織，了解該國於個人保護獨立監督體制及配套機制落實層面之相關經驗，作為我國推動成立個人資料保護委員會之參酌。並透過個人資料保護委員會籌備處首度與南韓相關機關、單位雙向交流之機會，建立往後委員會相關制度建立之交流、溝通及合作之聯繫管道。同時，期望汲取南韓等國家建立獨立機關及落實執法之相關經驗，作為評估我國獨立機關組織、執掌與監督機制建構之借鏡。

本次拜會單位，就執法監督層面，主要為南韓個人資料保護委員會（Personal Information Protection Commission, PIPC）及個人資料保護紛爭調解委員會（Personal Information Dispute Mediation Committee, PIDMC），以及依據總統令指定協助南韓個人資料保護法執法任務之專業機關：韓國網路振興院（Korea Internet & Security Agency, KISA）、受到 KISA 認證為目前南韓政府認可之個資保護認證制度－ISMS-P驗證機構的個人資料保護協會（Online Privacy Association, OPA），以及網羅南韓個人資料保護專家，依法建立個人保護長聯席會，且深入參與南韓個資法修訂等法制政策研擬之韓國個人資料專家協會（Korea Association of Personal Data Professionals, KAPP）。

為促進議題交流效率，本籌備處已於赴韓前先行將欲交流之具體議題提供韓方參考，受訪單位皆已明瞭臺灣現階段正為建立個人資料保護獨立專責機關而努力，表達期望本次參訪之後，未來有持續溝通與合作之機會。會議後部分單位並有提供進一步書面補充資料，以協助我方後續進一步了解其相關制度之運作情形。故本次參訪已順利達成初步建立相互了解與聯繫機會之目的，有助於往後我國法制與組織規劃、建置過程能有更深入具體之互動，並為往後個資保護獨立機關間之國際合作奠定基礎。

目錄

壹、考察緣起、目的與行程

一、緣起

我國個人資料保護法，自電腦處理個人資料保護法時代，即採取公務機關與非公務機關監督模式分流之作法，非公務機關部分現階段並仍處於目的事業主管機關分管之情形。依據憲法法庭 111 年憲判字第 13 號判決意旨，應於判決宣示之日起 3 年內建立個人資料保護之獨立監督機制，以增強個人資料蒐集、利用之合法性與可信度。而針對個人資料保護事項設置獨立機關，為目前國際主要國家與國際組織發展相關法令發展之趨勢。以歐盟為例，其於 2016 年 4 月通過一般個人資料保護規則(General Data Protection Regulation, GDPR)，並於 2018 年 5 月 25 日全面實施。其中 GDPR 第 51 條要求各成員國必須建立一個或多個獨立機關，以監督 GDPR 相關之實踐情形。各獨立機關並依據 GDPR 第 57 條規定，應進行適切之認知建構、法制與行政措施評估建議、執法落實、申訴協助、監督機關之合作、資訊分享、認證標準建構推動等各項為達成 GDPR 法制目標必要事宜。獨立專責機關之型態亦各有不同，有採取獨任制者，亦有採取委員會制者。以我國而言，基於現行個人資料保護法第 1-1 條第 1 項之規定，本法之主管機關為個人資料保護委員會，其方向應係採取委員會制之走向。而鄰近日本、南韓之個資保護獨立機關亦係採取委員會之性質，加上法制背景、分散監管歷史(如日本)、APEC 及全球 CBPR 論壇(Global CBPR Forum)參與以及皆曾嘗試/取得歐盟 GDPR 適足性之背景，使得日、韓之獨立機關架構、權責安排、實務運作與相關法制發展等，實值得進一步觀察，以作為我國獨立機關相關法令制度規劃之參考。

二、目的

本次考察適逢南韓已通過歐盟適足性認定，並於 2023 年 9 月就個人資料保護委員會等相關權限完成進一步之修法，故藉此機會拜訪南韓個人資料保護委員會及與其執法、立法相關之代表性單位或組織，了解該國於個人保護獨立監督體制及配套機制落實層面之相關經驗，作為我國推動成立個人資料保護委員會之參

酌。並透過個人資料保護委員會籌備處（以下簡稱籌備處）首度與南韓相關機關、單位雙向交流之機會，建立聯繫管道，為往後委員會相關制度建立之交流、溝通及合作，建立適切之管道。同時，期望汲取南韓等國家建立獨立機關及落實執法之相關經驗，作為評估我國獨立機關組織、執掌與監督機制建構之借鏡。

三、行程

本次考察規劃之拜會單位，就執法監督層面，主要拜會南韓個人資料保護委員會（Personal Information Protection Commission, PIPC）及個人資料保護紛爭調解委員會（The Personal Information Dispute Mediation Committee, PIDMC）。此外，基於個人資料保護法之規定及總統令之授權，韓國網路振興院（Korea Internet & Security Agency, KISA）於個人資料保護之外洩通報、侵害通報及就 PIPC 之案件調查協處層面，扮演極為重要之角色，同時亦為南韓法定資訊安全及個人資料保護標準（ISMS、ISMS-P）之認證及管理機構，故亦與之接洽拜訪，惟恰逢其所在地點及業務時程與其他單位較難配合，例外於實際參訪之前，於 7 月 17 日安排線上會議，進行相關議題交流。另於民間組織層面，則安排兼具民間驗證/標章機制推動經驗，且受 KISA 認證為 ISMS-P 驗證機構之個人資料保護協會（Online Privacy Association, OPA），以及網羅南韓個人資料保護專家，依法建立個人保護長聯席會並深入參與南韓個資法（於本報告後續簡稱個資法）修訂等法制政策研擬之韓國個人資料專家協會（Korea Association of Personal Data Professionals, KAPP）。

個人資料保護委員會籌備處考察行程表

日期	時間	拜會單位
7/17 (三)	下午 (視訊)	**韓國網路振興院** **Korea Internet & Security Agency, KISA**
7/23 (二)	啟程	
7/24 (三)	上午	**個人資料保護協會** **Online Privacy Association, OPA**
	下午	**駐韓國台北代表部**
7/25 (四)	上午	**韓國個人資料專家協會** **Korea Association of Personal Data Professionals, KAPP**
	下午	**1.個人資料保護委員會** **Personal Information Protection Commission, PIPC** **2.個人資料紛爭調解委員會** **The Personal Information Dispute Mediation Committee, PIDMC**
7/26 (五)	返程	

貳、會談情形

一、韓國網路振興院（Korea Internet & Security Agency, KISA）

(一)單位背景說明

韓國網路振興院（KISA）成立於 2009 年，現隸屬於南韓「科學技術資訊通信部」（과학기술정보통신부），原職司南韓 IPv4/IPv6 網域空間及國家級.kr 網域名稱之管理，後陸續負責南韓之網路安全、技術資格考試及數位隱私保護等相關事宜之推動。目前為南韓個人資料保護法第 34 條下經總統令（個人資料保護施行令第 40 條）指定之個人資料外洩通報之專門機構，亦為第 62 條規定，經 PIPA 指定為個人資料侵害舉報中心，故於個人資料保護之監督與執法，扮演極為重要之角色。

KISA 之預算來源主要來自政府挹注，PIPC 提供之預算占 KISA 總預算之 15%，就其機關組織來看，其目前業務層面之主要單位包括經營企劃部、數位威脅回應總部、個人資料安全利用總部、資訊安全產業總部以及數位安全支援中心，對於網路及數位資訊環境安全威脅層面有極為堅實之組織與專業人員（包含不同技術層面之專業團隊），故於本次參訪過程中，後續拜訪之單位包括 PIPA 及 OPA 皆有提及 KISA 於個資事故調查過程，於技術支援層面之重要性。

本次 KISA 之線上訪談，KISA 之受訪代表有個人資料合作組정태인（音譯：鄭泰仁）組長、ISMS 認證組박창열（音譯：朴昌烈）組長、人工智慧隱私組강혜영（音譯：姜慧英）研究員、個人資料調查團隊之公共調查組문홍식（音譯：文宏植）組長以及個人資料合作組국향（音譯：國香）組員。

(二)會談重點摘要

1. 侵害事故通報、調查協助實務

(1)個資侵害事故通報機制

A. KISA 針對侵害事故通報之受理，以線上通報為原則，但若使用網路困難，亦可接受透過郵寄或傳真方式之通報。

B. 侵害事故通報與外洩通報為分開的機制，侵害中心係負責個資外洩以外之個資侵害事故通報的受理。外洩事故則是例外的管道，係 KISA 與 PIPC 合作受理通報，此部分受理通報之類型包括駭客攻擊、作業疏失或故意洩露之情況等。

(2)外洩事故通報網站

外洩事故通報網站是由 PIPC 與 KISA 共同管理[1]。依據規定，發現外洩事件之機關或事業，有義務於 72 小時內進行通報。故 PIPC 可以從案件通報時，接收到外洩事件相關事實，即可以先進行分析評估與歸類，若有涉及技術分析而需要 KISA 協助的話，PIPC 會依據個資法關於請求專門機關協助之規定，對 KISA 提出請求，但最後仍是 PIPC 統籌處理及作成決定，故並非所有外洩事件皆由 PIPC 與 KISA 一起進行調查。

(3)有關金融等特別規定之個資外洩通報方式

原則上信用資料，銀行、保險公司、證券公司等金融機構向金融監督院、金融委員會進行通報；惟一般商業交易行為導致之信用資料外洩等事宜，則是回歸運用前述 PIPC 與 KISA 共同維運之網站進行通報。故就 KISA 而言，業務面之參與僅限於一般商業交易導致信用資料外洩之相關案件。

---

[1] 詳參 https://www.privacy.go.kr/front/main/main.do

2. ISMS-P 認證

A. 2018 年以前，係由 ISMS 與 PIMS 制度共存；2018 年之後，ISMS 及 PIMS 制度合併，而推出新的 ISMS-P 制度。ISMS-P 驗證標準係由 KISA 所訂定，並由科學技術資訊通信部以及 PIPC 兩個部門逐步將此驗證基準公布，成為南韓個資保護管理之公定基準。

B. ISMS-P 認證基準係於 ISMS 加上個人資料保護內容，故取得 ISMS-P 認證，等於已經同步取得 ISMS 之認證。事業若並未有對個資之處理，則僅需申請 ISMS 驗證即可，業務涉及個資保護層面，可再進一步申請 ISMS-P 驗證。

C. 推動 ISMS 義務化之歷程及推動 ISMS-P 義務化之必要

(a) 有關是否透過法律進行強制導入之要求，因為導入制度對於事業組織而言都是有相當的負擔，故南韓一開始推行相關驗證時，係採取自由導入與驗證之機制，但執行效果不彰。

(b) 後來才將 ISMS 制度義務化，於法律規定特定類型之事業組織，有義務導入 ISMS 並驗證通過。而 ISMS-P 目前尚未以法律規定義務化，故此部分之執行效果仍無法比擬 ISMS。故若臺灣要考慮推動相關制度，應要思考如何提高推行效能。

(c) 而是否一步到位將 ISMS-P 制度義務化之問題，南韓 ISMS 制度很早即義務化，刻正研議義務化事業單位取得 ISMS-P 之必要，惟 ISMS-P 之義務化有加重事業單位負擔之虞，故尚在研議中。

(4)其他驗證標準

目前僅有 ISMS-P 對應個資法之規定，但國際上標準(例：ISO 27701)亦有人導入驗證，但並非如 ISMS-P 是南韓國內認可符合個資法規定之標準。

3. 安全維護措施

(1)有關韓國是否有針對安全維護措施之相關規範或技術指引一節，個資法及其施行令皆針對個人資料處理者應採行措施以確保安全之部分訂定相關規定。

(2)個資法係於第 29 條，規定個人資料處理者必須依照施行令之規定採行必要之技術和管理措施，以確保安全，例如：制定內部管理計畫並保存相關存取紀錄，以防止個人資料遺失、被盜、洩漏、偽造、竄改或毀損之相關措施。施行令則規定於第 30 條，進一步對於所謂內部管理計畫、存取措施、安全之儲存與傳輸、紀錄儲存、程式之安裝/操作/定期更新與檢查、針對儲存設施之安全實體措施及其他可確保個人資料安全之措施加以規範。

4. 新興科技運用

(1)假名資訊支援平臺

A.「假名資訊支援平臺」[2]係由 KISA 維運提供假名處理方案、技術支援及假名處理，該平台目前由 KISA 進行假名資訊平臺之運營管理，主要係提供法律規範之說明、處理方式、解決方法以及監管機制。個人資料若要假名化，其類型十分多元，故並沒有固定之標準。

B. 每次個案會有 3 名專家組成審查小組，進行評估。此外，基於 AI 技術之發展，原來之假名資訊處理小組，目前亦投入 AI 隱私之處理，共計 7 名成員，其同時進行假名資訊處理與 AI 隱私事務。

(2)提升 AI 產品透明度或科學檢驗方法

KISA 刻正研議制定如何確保 AI 檢查方法及透明度之指引，而近年來，於特定服務當中取得當事人同意提供 AI 學習資料之情況已有所增長，但是若要針對過去之資料再度取得資料主體之同意有難度，因此必須要透過

[2] 詳參 https://dataprivacy.go.kr。

假名資料專用之機制刪除個人識別要素，方能提供使用，目前係以假名資訊處理準則作為基準進行處理。

5. 南韓推行 CBPR 情形

南韓事業單位取得 ISMS-P 認證後，易接續取得 CBPR 認證，故南韓目前係給予已通過 ISMS-P 驗證之事業免費申請 CBPR 驗證。截至 2024 年 7 月，韓國已有 13 家事業獲得 CBPR 之認證，而其認證機制之建構，亦是參考南韓事業熟悉之 ISMS-P 認證機制，以使事業易於準備。

6. 國際觀測

(1)KISA 於國際趨勢掌握之人力資源投入情形為何？

基本上對於國際趨勢層面有委託外部調查機構/研究單位協助進行，每年預算大約 5,000 萬韓圜(約新台幣 112 萬元)，KISA 內部則有 1 名員工擔任此業務之窗口。主要委託調查研究層面，包括個資教育、個資執法相關處分、案例之調查或統計等。

(2)KISA 於促進南韓個資事務跨境合作之角色與方向為何？

A. KISA 有參與相關之國際會議或組織，包含：全球隱私大會（Global Privacy Assembly, GPA）、亞太隱私機構組織（Asia Pacific Privacy Authorities, APPA）等，亦參與亞太經合會（Asia-Pacific Economic Cooperation, APEC）、經濟合作暨發展組織（Organisation for Economic Cooperation and Development, OECD）之轄下工作小組。

B. 國際業務之推動，主要係期望得以了解海外相關政策、機制之趨勢發展，並與國內利害關係人進行分享，同時向國際社會分享南韓推動個資保護之最佳實務，與海外相關組織建立合作體系。

7. 人才培育

(1) 就內部人員之培訓而言，其每年有制定年度教育訓練計畫，從領導、工作及共通能力層面規劃，實際訓練則委託外部專業培訓機構。

(2) 內部員工並不會被要求必須具備特定資格，但鼓勵同仁取得個人資料管理者（Certified Privacy Protection General, CPPG）或資訊保護管理系統認證審查員等資格，至於內部負責教育訓練業務之員工僅有 1 名。

(3)有關培養各領域個資保護人才、促進大眾個資保護意識等事宜，係從以下三方面著手：

A. 提高意識：主要針對中小學學生、身心障礙者或老年人等弱勢族群。內部投入人力為 1 人，年預算共計 3.6 億韓圜。

B. 能力強化：對象則為公務機關、中小企業之個人資料處理者（包括負責人、個資長(Chief Privacy Officers, CPO)或儲備之 CPO 等），進行線上或線下之教育，內部人力投入亦為 1 人，年預算共計 4.7 億韓圜。主要課程包括分級的訓練（基礎或實務課程）、個人資料專業課程（公共機構、違法案件課程、新技術課程）、CPO 能力密集之培訓。

C. 培養人才：主要是透過配合指定之資訊專門大學進行人才培養，截至 2024 年共有 5 所大學參與。內部人力投入為 1 人，預算 25 億韓圜，主要為個人資料領域之專業培訓課程，KISA 係以產學合作方式提供協助。

二、個人資料保護協會（Online Privacy Association, OPA）

(一)單位背景說明

OPA 係南韓個資保護自律認證制度建立、個人資料保護教育及意識推廣之機構。OPA 於 2011 年獲政府許可成立，主要服務對象為通信業者，於 2012 年建立個人資料保護自律監控中心，於 2018 年整合電信領域個資保護自律機制，並於 2020 年受認證指定，成為資訊安全管理制度（Information Security Management System，ISMS）之驗證機構。

OPA 由會長領導，其次為副會長襄助綜理組織業務，總部下設管理支援、政策商業、自律規劃及商業、隱私認證檢驗及授證等四單位。OPA 目前服務之事業共計 55 家，包含電信、線上購物及安全等領域。

就 OPA 之業務主要分為五大部分，與本籌備處業務關聯度較高者為個資保護認證計畫：

1. 個人資料保護自律計畫
   主要包括協助電信業者進行個資保護之自律推動、協助購物商場賣家個資保護之現場稽核、針對網路購物產業自律之公私協力合作等。

2. 電信領域個資保護相關合作
   主要包括設置及營運自主監控中心，例如監督對非法使用個人資料情況之補償等。

3. 個人資料保護認證計畫
   主要包括資訊安全管理制度（ISMS）以及個人資料管理制度（ISMS-P）之驗證、OPA 自主推動與維運，針對事業個資保護等級之標章驗證制度，包括 ePrivacy、ePrivacyPlus 以及 Privacy 制度。

4. 政府補助或委託相關業務
   主要包括協助個資保護委員會之調查人員培訓、執法調查

之協處、個資保護利用情形之統計調查以及網路資訊傳輸加密監控與精進之相關業務。

5. 位置資訊業務支援相關事務（法遵及精進措施等）
與位址資訊相關事業（例如蒐集位置資料之業者）合作進行調查分析，以及法遵相關研究。

本次 OPA 拜訪，會議開始前該會之권미혁（音譯：權美赫，前民主黨國會議員）副會長及박찬휘（音譯：朴燦輝）總管本部長前來致意。實際受訪代表有資訊安全認證안준모（音譯：安俊謀）總監、隱私認證組김희수（音譯：金熙秀）組長、審查認證組김정우（音譯：金政宇次長）以及營運支援組박수진（音譯：朴秀珍）次長。

(二)會談重點摘要

個資保護認證計畫包含 ISMS 及 ISMS-P 驗證制度管理及授證、推動 PRIVACY 認證標章。

1. 關於 ISMS 及 ISMS-P 驗證

ISMS 主要針對公、私部門與個人進行，提供教育訓練。另外有蒐集位址資料，跟產業進行合作，提供統計調查服務，以受政府委託進行研究為主，少數為民間商業使用。

(1) 驗證種類及認證方式

A. 目前官方認可之管理制度，於資訊安全層面為 ISMS，主管機關為科學技術資訊通信部，個人資料管理層面為 ISMS-P，主管機關為個人資料保護委員會。

B. 目前對於 ISMS 及 ISMS-P 之驗證標準，除與金融及信用資料相關之標準，由金融安全研究所(Financial Security Institute, FSI)訂定外，其餘皆由 KISA 訂定頒布。

C. 經 KISA 目前已認證指定 4 個驗證機構，包含 OPA、南韓資通信協會(Korea Association for ICT

Promotion, KAIT)、通信科技協會(Telecommunications Technology Association, TTA)、下世代資訊安全認證院(Next-generation Information Security Certification，NISC)等，發證仍由 FSI 及 KISA 授予。

(2) 驗證基準與效期

A. ISMS 資訊安全驗證基準共計 80 個，其中 16 個為管理制度之驗證基準，64 個為保護方式之驗證基準。ISMS-P 個資管理驗證基準，則是於 ISMS 之 80 個驗證基準上再加上21個與個資保護相關之驗證基準(由 KISA 自主加入)，總共 101 個基準。

B. 兩者驗證有效期限皆為 3 年，第一次通過驗證後每年會有一次基礎之審查，3 年再為一次更新之審查，每3年為一個週期，現階段已通過驗證共計 1090 案。

圖表 貳-1 ISMS 及 ISMS-P 認證標章

(3) 驗證對象

A. ISMS 驗證之法源依據為資訊通訊網路法第 47 條，主要針對具有法定義務需進行導入驗證的業者包括資通訊網絡服務供應商（Information and Communication Network Service Provider, ISP）、網路資料中心（Internet Data Center, IDC）、醫院、學校以及具備一定規模之資通訊服務提供事業（前一年度銷售額超過 100 億韓圜之事業或於前一年度最後三個月每日平均使用者達 1 百萬者），需強制導入並驗證通過，其餘事業則可自行決定是否導入並取得驗證。

B. ISMS-P 之驗證法源依據則為個人資料保護法第 32-

2 條，為非強制之驗證，由事業自主決定是否導入及取得驗證。

(4) 驗證範圍

ISMS 驗證範圍，主要著重於提供服務之組織、人員、場所及基礎設施。ISMS-P 則加強針對組織、人員以及基礎設施中涉及個人資料處理層面之調查。

(5) 取得認證家數

OPA 在內的四個 ISMS 驗證機關，驗證通過 ISMS 的機構共有 1090 家。ISMS-P 家數約 1090 家的 25~30%，二認證不得直接轉換，須另行申請認證取得。

2. PRIVACY 認證標章

(1) 性質與層級化驗證

A. PRIVACY 為民間建置之事業自主認證系統，用於評價事業單位的個資保護水準。目前 OPA 已完成 150 項授證，公部門 92 項、私部門 58 項，包含購物(例：samsung, Coupang)遊戲(例：NEXON)及公部門(例：韓國就業資訊中心 KEIS)等。

B. PRIVACY 由基礎至嚴格分為以下三級，ePRIVACY 驗證進行期間為一天完成，較為嚴格之 PRIVACY 則 3 至 4 日：

(a) ePrivacy：業者的網頁及管理者頁面之驗證（主要為小型企業）。

(b) ePrivacy+：針對網頁以及網頁相關之系統及基礎架構技術之驗證。

(c) PRIVACY：相較 ePrivacy 及 ePrivacy+僅就網頁進行檢視，PRIVACY 就整體實質部分進行評估，聚焦於醫療、供應商、預約管理系統等特定業者的資訊系統及管理制度，與 ISMS-P 較為近似。

圖表 貳-2 PRIVACY 系列驗證標章

(2) 驗證基準及與 ISMS-P 之差異

PRIVACY 制度主要係依據個資法第 13 條關於促進自律及支持個資保護認證標章之導入與實施等相關規定所訂定，現階段 OPA 為唯一的民間認證單位。而 PRIVACY 制度雖較類似 ISMS-P，但兩者之間無法轉換，事業可選擇其一導入，然因為 ISMS-P 有其法律依據，故選擇導入 ISMS-P 之事業比例較高，其費用亦較高，收費基準係由 KISA 訂定之。至於標準之更新，主要對應個資法，若個資法有修法之情形，即會評估調整驗證基準。

(3) 效期、通過效果與現況

e-Privacy 為每年驗證一次，e-Privacy PLUS 及 Privacy 之效期與驗證頻率與 ISMS-P 相同，皆為 3 年 1 期，每年有基本之事後稽核，3 年後進行更新驗證。現階段通過 e-Privacy、e-Privacy PLUS 或 Privacy 驗證者，共計有 150 個公務及非公務機關，其中 92 個為公務機關，非公務機關較具代表性者為三星集團等。

(4) 其他

A. 對認證事業提供之服務

PRIVACY 對業者提供的服務包括教育訓練，受罰時可降低金額（10%），協助監管事業的委外單位。

B. 取得認證的優點

為鼓勵事業導入、建置並申請包括 ISMS-P 或 PRIVACY 非強制之個人資料管理制度/標章，南韓 PIPC 於個資法之裁罰基準面，有將是否通過相關制度與驗證，規範適當比例之裁罰減免：

(a) PIPC 調查涉有外洩事業時，若受調查者有取得認證，可降低處罰金額，ISMS 認證降低 20%，PRIVACY 是 10%；降低金額的百分比有主管機關指引作為法定依據。

(b) 經查，南韓 PIPC 因應 2023 年個資法修法，修正公布之「違反個人資料保護法之裁罰標準」（개인정보보호법위반에대한과태료부과기준）中，針對罰鍰減輕層面，就組織為保護個人資料之努力程度，提出可減輕裁罰之相關事由。其中違法者若有取得個資法第 32-2 條規定之 ISMS-P 包括有效的 PIMS 認證，可減少 40%以內之罰鍰金額；行為人若非資訊通訊網路法第 47 條第 2 款指定必須通過 ISMS 驗證之事業，而通過 ISMS 驗證者，得減少 20%以內之罰鍰；若係獲得個人資料保護相關國際認證（ISO27701、ISO27001、BS10012）等，得減少 20%以內之罰鍰；至於行為人若係取得民間自律標章認證，如 e-Privacy PLUS 或 Privacy 認證，則得減少 10%以內之罰鍰。罰鍰減免之公示，使得事業導入並通過相關驗證制度，得以作為投入個資保護與管理之證明，對事業投入導入得收鼓勵之效。

證照取得	最高減免比率(%)
ISMS-P	40
ISMS	20
ISO 27701	20
ISO 27001、BS10012	20
PRIVACY 認證系統	10
註:前述減免比率僅適用於認證範圍內發生違規行為之個人資料處理系統。若同時適用二個以上認證系統，則取高者。	

(c) 除了罰鍰之減輕外，PIPC 也鼓勵已取得 ISMS 驗證通過之事業或組織，可以免手續費取得 ISMS-P 之驗證，惟若是 Privacy 驗證要轉 ISMS-P，則不得減免。

C. 驗證人員來源及資格

(a) 有關 OPA 之驗證專業人員培養及個案驗證規劃與人員安排，ISMS、ISMS-P 之驗證專業人員人才庫，係登記於 KISA，驗證由人才庫的專家選任組成，目前共計有 150 名驗證人員。

(b) 若要列入 KISA 驗證人員人才庫，必須具備 5 至 6 年個資事務相關經驗，並通過考試取得資格。若有申請驗證案件，係由 KISA 收取後，指定驗證機構主辦，驗證機構如 OPA 會指派一人擔任驗證組之組長，其餘驗證員則由 KISA 自人才庫登錄之 150 名驗證員當中指派，由 OPA 組長帶隊進行驗證審查。每次驗證之驗證小組大約 3-4 名驗證員，會視受驗證單位之情形調整驗證小組之規模，最多可能會到 7 位驗證員。

(c) PRIVACY 認證之驗證員基本上為 OPA 之內部職員。全會 35 人當中，有 5 位可以執行 Privacy 之標章驗證，另有 5 位可以執行 ISMS(等)之審查。

D. 個資外洩調查

發生個資外洩事故時，基本上係由 PIPC 主導案件之調查，惟若發生事故之事業，係通過 OPA 驗證之事業，則 PIPC 可能會請 OPA 前往說明該事業通過驗證之審查流程。OPA 對於個資外洩之調查並無主導權限，係配合 PIPC 要求，指派相關專業調查員協助政府調查之進行。

3. 金融機構之資料驗證

ISMS-P 之 101 項驗證基準也可適用於金融資料，但驗證

之方式不同，且對金融機構而言，其相關法令並未有關於驗證標準之明確規定，故金融機構若要導入，屬於自律性質。OPA 不會對金融機構予以驗證，而係由金融相關協會（如：FSI）主導；此外，金融機構尚有電子交易相關之基準，則屬於其他法領域之範圍，亦非 OPA 可處理之範圍。

4. 提高事業參與驗證制度比率

針對如何拉高事業參與制度驗證之比率層面，OPA 表示，每個國家環境不同，故未必可以提供實質建議。就南韓而言，為何會建立 ISMS 及 ISMS-P 制度，前者並部分依法強制導入，是因為曾經發生過大規模之事故。而透過法律予以義務化，確實也促使更多事業參與並通過驗證。而目前通過 ISMS-P 之事業總數，大約是通過 ISMS 事業之 20% 至 25%，也就是大約 300 家事業。兩者之間不能直接進行轉換，故即使已通過 ISMS 驗證，仍需另外申請 ISMS-P 驗證。

圖表 貳-3 OPA 考察合照

三、韓國個人資料專家協會（Korea Association of Personal Data Professionals, KAPP）

(一)單位背景說明

KAPP 成立於 2020 年，會員為南韓個人資料保護法制或實務相關專家，目前會員共計 300 至 330 名左右，涵蓋教授、律師、公務員、個資保護負責人／個資長（Chief Privacy Officer, CPO）、與實務上從事個人資料處理業務之人，屬於技術性、法律性、專門性之專家團體。

KAPP 協會主要係針對個人資料保護之政策或法制積極參與，其中受訪之李顧問（Byungnam Lee）並為甫自 PIPC 退休之專家，曾參與 PIPC 之設立及個資法之修法。除法制政策之參與外，該組織並投入事業、個資保護專家及政府間之溝通、人員之教育訓練（自基礎訓練至專業訓練）、個人資料保護相關之研究與學術活動、書籍與期刊出版、國際合作與相關專案之規劃與執行，同時其並成立 K-CPO（韓國 CPO 聯席會/理事會），為韓國第一個依據新修訂之個資法第 31 條第 7 款成立之 CPO 聯席會，係於南韓個資保護法制建構與實務推展極為積極之民間專家組織。

本次 KAPP 受訪之代表為 Kim&Chang 法律事務所 이병남（音譯：李秉南）資深顧問，及加昌大學法學院최경진教授（崔景津），李資深顧問為南韓個資保護政策規劃顧問，為南韓個資保護政策最頂尖的專家及催生 PIPC 的主要推動者之一；崔教授目前為 KAPP 之會長，為南韓於人工智慧、資料、隱私方面長期投入學術及實務實踐之專家。李資深顧問及崔教授皆有參與南韓個人資料保護法之起草及修訂。

(二)會談重點摘要

1. KAPP 與政府單位之互動

(1) KAPP 與公部門間之互動，主要為法制政策研議相關部分之參與。因為 KAPP 幾乎涵蓋南韓主要之個人資料保護專家，故會受邀參與政策、法制研議，或提供意見。

(2) 李顧問表示，去年（2023 年）大致就個資法完成 76%的修訂，於準備過程即已經跟各產業界、市民團體、產業團體、消費者團體、專家學者與國會等，廣泛蒐集對修法之意見，其後則召集 10 位個資專家作為 PIPC 之外部專家（大部分亦為協會之會員)與 PIPC 共同進行法案之修訂，並需要 20 名國會議員參與協議，歷經相當充分的討論。而產業、專家、市民團體等所提出之各方意見，本身亦有相當之衝突，PIPC 即須努力從不同意見當中找到平衡點，故從意見徵詢到最後完成立法，共計花費 2 年 6 個月的日程。

(3) 關於個資法罰則當中之銷售額門檻，基本上係修法之過程中，KAPP 協助蒐集許多產業界之銷售額資料，供 PIPC 評估應如何設定銷售額界線。至於為何個資法罰則比例為 3%，則主要是參考 GDPR 兩種罰則比例之 2%及 4%，取中間數。至於實際裁罰時，個案所涉事業必須切實提供實際的銷售額，不得提供錯誤之資訊。

2. 專業人員教育訓練

(1) 有關訓練類型及經費來源，基本上 KAPP 所推動之教育訓練，並不限於專業之教育訓練，而係從基礎之認知至專業之教育訓練皆有所推動。政府並沒有提供經費支持，主要經費來源為會員繳交之會費。

(2) 至於專業人員訓練，應查包含個資管理人員、專家、個資處理者、CPO 及 DPO 等人員，其訓練現階段並未提供國家級之證照，但 KAPP 目前已經在與 PIPC 討論，對於未來最高層級之 CPO，是否應給予相當之資格證明。此外，去年修法涉及之 CCTV 監管，其專業人員是否應給予相

關之資格證，亦在評估籌備中。

3. 南韓個資長委員會(Korea CPO Council, K-CPO)

有關設置 K-CPO 之主要功能、運作及與 PIPC 之關係，基本上事業內部之 CPO，本身可自發性的成立一個類似協會的組織，並非強制要求的義務，但可以透過這樣的協會，彼此間進行交流，並提供相關修法建議給 PIPC。此類協會成立係依據個資法第 31 條之規定，並不限於一個，據了解，目前尚有其他的協會組織準備中，只是目前尚未正式成立公布。

4. 如何確保企業遵守非強制性措施

針對近期南韓公布之人工智慧個資保護指引、產品事前審查制度，皆非強制性，此類非強制之措施，如何確定企業是否遵守，以及相關制度如何推動一節，目前採用大語言模型人工智慧技術者，多數為全球性事業，諸如 Meta、Google 等。現階段 PIPC 對於前述全球性事業之資料運用，尤其針對資料學習與服務之提供層面，有違反南韓個人資料保護相關規定之虞者，有提出相當之改善勸告與指正。至於這些全球性企業以外之其他事業，包括許多網路上之服務也有 AI 之應用，PIPC 所提出之指引，主要係針對此類 AI 服務，使之了解應如何提供服務，若有疑問，可以要求事前審查，但並非所有的服務提供皆有提出事前審查的必要。相關指引目前只是起步，後續應該還會有針對 AI 風險評估之相關指引提出。

5. 事業進行個資影響評估是否需經 PIPC 審查

目前 PIPC 針對風險評估之模型尚在開發階段，預計今年底會完成風險評估模型。而目前已提供 AI 服務之公司，包括 Open AI、Google、Meta 以及南韓國內之 Never 等公司，現階段係由 PIPC 進行一次性的事前審查，透過此一審查即會提供該事業改善勸告等建議，事業若未改善則會被處以過怠金。只是現階段之風險評估屬於自律性質，未來 PIPC 完成風險評估模型後，是否仍維持自律或會走向強制，尚未有明確的政策決定。

6. 申請歐盟適足性認定

有關南韓過往申請適足性認定過程中歐盟對南韓最主要之要求，李顧問表示，歐盟對南韓最主要之要求，為必須要有獨立機關，以及民間資料一定要入法。南韓個資委員會雖然過去也存在，但並非獨立機關，而僅係提供諮詢建議之機關，目前之 PIPC，方為因應適足性認定設置之獨立機關。

7. 人工智慧監理

有關南韓是否具備類似新加坡之 AI 評測中心及 AI 法案之發展一節，目前南韓主要係由科學技術資訊通信部負責處理 AI 相關議題，預計於 AI 法制通過後將建立研究所，並推動與美國國家標準暨技術研究院(National Institute of Standards and Technology, NIST)合作。而韓國進行中之 AI 法案，基本上與歐盟人工智慧法之規範方向差異不大，惟南韓之規範將更著重於高風險 AI 之監理。

8. CCTV 之規範

有關南韓因應個資法就 CCTV 規範之落實，有設置 CCTV 管制中心，是否亦將與 AI 法制落實相關聯一節，南韓政府建置之 CCTV 管制中心，必須是有取得資格證者方可進入，但此一資格證為獨立之資格證，與 AI 資格證無關，因 AI 相關資格證照仍在發展中。而現階段 CCTV 中心之設置，並未有法源依據，主要係由各地方自治團體及警察廳進行維運，資格證制度主要就是期望可以管制相關人才。而 PIPC 目前亦在規劃於未來就 CCTV 人才之相關立法。

圖表 貳-4 KAPP 考察合照

圖表 貳-5 KAPP 考察會議進行

四、個人資料保護委員會（Personal Information Protection Commission, PIPC）、個人資料紛爭調解委員會（The Personal Information Dispute Mediation Committee, PIDMC）

(一)單位背景說明

PIPC 為目前南韓處理個人資料保護相關事務之中央獨立機關，其職責係完善個人資料保護相關法律，建立和執行政策、制度及計畫，調查和處理侵害行為，處理申訴、權利救濟、調解糾紛，與國際個人資料保護機關進行法律、政策、制度交流與合作，並進行實際狀況下之調查研究、技術發展教育、宣傳與傳播、專業人員培訓等相關事務。有主任委員一人代表行使職權，主持保護委員會會議，並主管有關事務。委員任期共計三年，連選僅能連任一次，退任時必須立即任命或委任新的委員，被任命或被指定為繼任者之委員，其任期重新開始計算。個資法並於第 7 條之 9 明定應經過保護委員會審議決定之 16 款事項，主要囊括對於公務機關相關法令、政策涉及個資侵害要因之評價、公務機關基本計畫及施行計畫審議、與個資相關政策/制度/法令修正事項、個資目的外利用禁止、跨境傳輸禁止、影響評估審議、罰鍰、勸告、改善、糾正、告發、懲戒等事項、過怠金課予之相關事項、處分結果公布或其他依個資法或其他法令須由委員會決議之事項等。委員會下設置相關事務處理單位，支援委員會相關政策、執法任務之執行。

PIDMC 為依據個資法第 40 條及施行令第 49 條設置之委員會，設置目的在於得以方便、即時、便捷及妥善的解決因個人資料之處理利用所產生的紛爭。其總共有 30 名成員，包括一名主任委員，委員則由當然委員及指定委員所組成。所謂當然委員為國家機關依據施行令第 48 條之 14 於保護委員會之高級公務人員中指定之人員；指定委員，則由 PIDMC 之主任委員自符合個資法第 40 條第 3 項各款規定之人員中指定之。故可能包括曾經擔任個人資料保護工作之中央機關高級公務人員或在公共部門或相關部門擔任過類似職務之人員，或現在

或曾經擔任大學認可研究機構副教授以上或同等職位之人，或現在或曾經擔任法官、檢查官或律師之人，或由個資保護相關民間組織或消費者團體推薦之人，或擔任獲曾經擔任由個人資料處理者組成之商業組織的高階主管者。

本次考察 PIPC 及 PIDMC 係共同參與訪談會議，PIPC 主要係由職司國際合作之國際合作擔當辦公室主管及成員受訪，出席者包括國際合作擔當官최윤정律師（音譯：崔允靜）、國際合作擔當辦公室정유진（音譯：鄭宥珍）事務官、박선업（音譯：朴善業）事務官、新技術個人資料科김지영（音譯：金智英）事務官、調查調解局調查總管課나일청（音譯：羅日青）行政事務官以及調查調解局爭議調解課김용학（音譯：金龍學）書記官。

(二)會談重點摘要

■ PIPC 組織及業務運作實務

1.PIPC 委員會成員之組成及專業人才培育

(1) PIPC 成員組成及人才招聘方式

PIPC 組織成員包含法律背景及工科背景，法律層面包括法律系畢業之人員或律師，原則上需要通過公務人員資格考試，雖未要求須具備特定之專業證照，惟有編列相關預算支持成員取得證照。於特定領域人才需要時，會進行特別招聘，對象包括目前現職的公務人員或以契約約聘，前者將採取機關借調的方式進行，其薪資等預算經費來自國家整體公務員薪資預算；若透過契約約聘，則其所需之費用，需以 PIPC 本身之預算支應。

(2) 個資外洩調查業務之實務執行及人才培訓方式

A. PIPC 之調查業務均由公務員執行，惟涉及特定專業領域之調查，將視需求請 KISA 協助。負責調查之公務人員職培訓，係由 PIPC 會制定教育訓練計畫，由 KISA 執行訓練，現階段共有 30 名調查人員，均為隸屬 PIPC

之公務人員。

B. PIPC 對個資外洩調查人員之培訓訂有訓練計畫，「2024 年個人資料保護委員會調查員能力建構訓練計畫」(2024 년 개인정보위 조사관 역량 강화 교육 계획)，包含組織內部及外部之人才培訓。

(a)內部培訓：

主要分享調查實際或處置之案例，包括調查工作技巧之分享，或共同參與委員培訓之課程，並進行案例分析之討論，針對關鍵之法律原則及決策與委員會交流分析，對於新進之調查人員，並會安排有經驗之調查人員陪同進行實地調查。PIPC 支持相關人員之持續學習，包括取得相關認證，例如資訊安全工程或個人資料相關認證等。

(b)外部培訓：

以專門講座、相關認證課程為主，目的在強化調查人員的專業人力。包括針對專業技術、法律、或實際業務領域、調查工作之專題講座及教材之提供、新科技領域知識、趨勢之傳遞（如行業發展趨勢、暗黑模式等等）、得用於實務工作之培訓，以及支持相關認證之取得。計畫當中並指出，長期而言，尤其 2026 年之後，應該要推行具有一定年限工作經驗者須取得相關認證之要求。同時亦將舉辦調查部門全體職員皆能參加之研討會，以了解技術之動向、分享資訊並進行職員間之交流。

2.與其他機關/組織之互動關係與執法合作

(1) 有關 PIPC 如何協助公部門培育 CPO 人才一節，目前針對一定規模以上民間或公務機關，要求必須指定 CPO，而 CPO 之訓練基本上為獨立之制度，定期舉辦，並於大學推動個人資料保護相關學科。

(2) 有關 PIPC 與其他部會或組織之合作模式，個資法明定 PIPC 需要有其他專門部會協助時，部會即有提供協助義務，例如 My data 制度即為跨部門協力進行，PIPC 係與

法務部、行政安全部、金融委員會、科學技術資訊通信部與福祉部合作；另有 AI 技術之相關議題，PIPC 亦與科學技術資訊通信部合作。

(3) 個資侵害調查若有必要請機關協助，基本上依據個資法之規定，機關皆會配合協助，若有拒絕提供協助之情事，則會對拒絕協助之機關課予行政罰鍰，大約是 2000 萬韓幣之罰鍰。

3.法定職權委託實務

個資法第 68 條法定職權委託之單位就是 KISA，有編列預算供 KISA 執行。此外可能依據第 63 條規請地方政府協助，例如新冠疫情期間涉及出入填寫名單之相關事務，即是委託地方政府協助。

4.個資保護基本計畫

A. 中央行政機關

PIPC 依據個資法之規定，每三年會制定一部個資保護基本計畫，再由各中央行政機關依據該基本計畫制定各單位之實施計畫。PIPC 透由委員會審議該實施計畫及其執行之情況。此部分只有針對中央之行政機關的實施計畫，並未包括非公務機關。

B. 地方自治團體

地方自治團體層面，則會有其內部對於個人資料保護管理之執行方法，PIPC 並不會介入。此部分可能係因為中央之行政安全部有制定相關實施計畫，讓地方自治團體得以依據行政安全部之實施計畫落實執行。亦即行政安全部有依法指導地方自治團體之角色，而行政安全部依據其已通過之實施計畫指導地方自治團體，地方自治團體再據以規劃其計畫，各該計畫及落實情況，可能係由行政安全部審議。行政安全部基本上有兩個角色，其一為管理所有地方政府，其二為災難救助、應變與管理。

5.個人資料管理水準診斷

(1) 2008 年開始對於公務部門即有所謂之個人資料管理水準診斷，2023 年修法於今年（2024 年）實施之規範強化此一診斷，稱為個資管理水準評估，分為上、中、下三級。進行此一評估後，PIPC 會給受評估機關改善意見，並請機關提交改善方案，PIPC 並會予以監督，也列入機關年終考核，因此對機關很重要。而若機關發生外洩情事，PIPC 前往調查，並予以減分。

(2) 設計對公務機關風險評估之規制，主要原因在於公務機關(含中央機關與地方自治團體)可以依據法律規範蒐集許多敏感資料，因此，相較於民間團體會有更多嚴格或強制性的要求。

(3) 至於必須接受影響評估之範圍，就公務機關部分，除中央及地方自治團體外，還包括領有政府預算的團體，亦屬於影響評估的範圍。目前約計 1432 個機關，PIPC 實際 PIPC 執行審查之人力為 2 人，KISA 另支援 2 位人力，並有透過預算委外進行審查，委外人數尚待確認。外部評估專家則有教授、律師等共計 100 名。原則上會先蒐集相關資料進行審查，發現真的有問題，KISA 會再派 3 名人員進行現場審查。

(4) 審查結果原則上會讓機關首長知悉，讓機關首長可以進行內部的審視。此一評分將會影響到各機關之年度考核，且結果會公開，以 ABCD 等級分類，故各機關會努力爭取，與預算多寡無關。

(5) 現階段依法有義務受影響評估之機關為處理個人資料超過 100 萬名以上的，或內部外部傳輸資料有達 50 萬名以上，或公務機關有利用或蒐集 5 萬名以上敏感資料者（個資法施行令第 35 條），即一定需要做影響評估。指定影響評估機構共計 14 個機構，指定條件規定於個資法施行令第 36 條有明確規範。

6.查核、調查實務與罰則

(1) 南韓之個資法效力涵蓋 350 萬個公務及非公務機關，對為

數眾多的適用對象，平時並沒有分級查核機制，僅就侵害或外洩事件會看是否違法，以及法律規定的罰則進行裁罰。

(2) 外洩事故原則上是接獲通報後進行調查，並不會自發性進行調查，若自發性調查屬於查檢，並非由調查組負責。除了發生外洩事故外，違反法律規範之侵害或有侵害之虞部分也會進行調查。而除了透過通報啟動調查外，也可能因為輿論、國會議員之要求而進行調查。

(3) 個資外洩事故中，實際案例經調查出現根因不明之情況很少見，大部分情形可以找到原因，因為調查過程會極為仔細的將系統完整的搜查一遍，此部分會由 KISA 進行。

(4) 就調查人力部分，現階段調查官有 30 名，分散於四個組，分組先以線上與線下區隔，線下再分公共機關、非公共機關；線上則可以區分成一般網路業者（線上網站），以及手機 APP 使用平台(例如阿里/淘寶，會列入 APP 平台)，並分為調查一到四課。

(5) 至於是否無論規模大小之外洩事故皆會進行調查一節，原則上不會按照規模來判斷是否啟動調查，而是會先去評估是否真的是外洩事件，例如只是不小心發錯 email 或發錯群組，並非外洩事故，這些會於案件受理時就進行事前瞭解，有侵害才會去進行調查。而部分案件為警察機關負責，例如個人資料遭到冒用，此部分 PIPC 則不會進行調查。涉及暗網駭客銷售個資的類型，通常是警方已經會介入調查，PIPC 主要調查事業內部個資管理的狀況。

(6) PIPC 網頁上可查詢及下載「個人資料保護委員會的調查暨處分相關規定」（개인정보보호위원회의조사및처분에관한규정）其中第 5 條之 2 即有列出不啟動調查之情形，例如檢舉人取消檢舉、資料不足判斷無法啟動調查、申報案件與已辦理案件相同（同一案件判斷）、案件與個資法無關、明確無違法情事、被檢舉人死亡或已受清算而經判斷無法進行調查等。受理情形會於網頁上公布，除網頁說明情況外，亦會就個案判斷調查之必要性。

(7)若有事件決定要進行調查，會先進行書面審理，再派員到現場確認現場情況，以進行結果分析，如此就會有基礎的案件事實與結果概要。會事先通知可能受到裁罰的單位，請其表示意見，之後製作一個審議案資料，提交九位委員組成的委員會進行審議並做成審議決定。原則上可能會課以行政罰鍰，若有異議則可提起行政訴訟。

7.個資侵害事故調查程序

(1)個人資料受到侵害之當事人，法定有兩個救濟流程，其一為侵害申告，此一流程類似於向警察機關告訴告發，其二為爭議調解，類似於民事訴訟之賠償，當事人可以選擇其一程序進行，或可同時進行。

(2)侵害申告部分，規範為個資法第 68 條，受理機關是 KISA，會由 KISA 就受理案件進行事先審查，此部分不涉及賠償的問題。

(3)至於通報義務規範於個資法第 34 條及施行令第 39 條，基本上並無所謂之標準， 若當事人想要獲得賠償，即須提出紛爭處理之申請。可申請紛爭處理者並不限於受侵害之當事人本人，若有其他機關發現有當事人個資受到侵害，皆可提出申請。

(4)有關 PIPC 與 KISA 之分工層面，最終作出結果的是 PIPC，涉及調查及技術層面由 KISA 介入參與。KISA 有三調查組，若 PIPC 調查官認為需要技術資源就會對 KISA 提出請求

8.安全維護義務要求

基本上安全維護義務之要求無法以事業之規模進行分類，只要涉及個資處理即須適用個資法。只有針對資料主體數、銷售額等，方有進一步規定上之差別。

9.對公務機關之現場調查

對於公務機關之現場調查通常會有 PIPC 之調查官 1 名，以及 KISA 之調查官 1 名。會視實際調查情況增加調整。調查只會針對應受調查之機關，並不會再對其上級機關進行調查。至

於國會等具憲法地位之機關（參考個資法第 2 條）法律對其並沒有特別的規定，仍與其他公務機關相同接受調查。

10.行政裁罰

(1) 韓國個資法進行行政裁罰金額計算之衡量因素或計算方式，包括舊法之徵收標準、評估標準，以及修法後之相關評估標準。

(2) 韓國的行政罰有兩個制度，其一為過徵金（不正行為之罰款），其二為過怠料（單純之行政罰鍰）。就判斷過徵金部分有訂定細部標準，依據違反行為之嚴重性，分為 4 個等級程度，非常重大、重大、普通、較輕等，依據該標準計算金額。若企業受害當事人有協議賠償，則過徵金或過怠料可有 30%的減免。

(3)2023 年 9 月 15 日修法以前對於線下之業者，只有發生敏感個資之外洩，方會課予 3%之過徵金，否則僅會課予過怠料；而線上業者只要有個資外洩，就會課予 3%之過徵金及過怠料。修法之後，即不再區分線上或線下，只要有個資外洩，無論是否為敏感個資，一律課予 3%之過徵金及過怠料。

11.國際合作及國際觀測

A. 國際合作

(a) PIPC 就國際合作部分，即是由國際合作辦公室執掌，而所謂之國際事務，主要就是參加全球性的各項個人資料保護委員會相關會議。

(b) 分工層面，基本上擔負國際合作任務的組別，會將所瞭解之海外動態與研究，提供其他業務單位交流。對於涉及個資保護相關或數位貿易往來事宜，則由國際合作小組負責與其他國家進行交流。

B. 國際觀測

(a) PIPC 有編列預算委外進行分析研究與調查，包括透過定期委外機制進行每週國際動向之搜尋及統計。國外規範層面也是持續觀察與更新，會產出相關之報告，部分用於內部業務討論之需要，若評估為可公開之內

容，則會置放於 PIPC 網站。PIPC 並未有常態之統計作業，只有於必要時才會以個案需求進行相關評估或統計。

(b)PIPC 之國際合作部門也會參與各項國際性會議，包括 APEC、GPA、IAPP、APPA 之相關會議等，可以透過國際會議與其他國家進行交流，掌握國際的動向。

12.新興科技因應

(1)PIPC 現階段針對新興技術之因應主要分三部：影像資訊、廣告投放及生物特徵，針對此三類情況進行隱私強化技術（PETs）之運用及推動。

(2)人工智慧

A. 2023 年成立人工智慧小組，現階段主要任務是進行各項指引之研議發布，並予民間團體充分合作交流，以面對 AI 難以預測之發展。

B. AI 小組目前預計將發布 6 份指引，繼本年 7 月發布「AI 開發及服務的個人資料處理指南」後，下半年將陸續發布相關文件，包括風險的指引。

C. 「AI 開發及服務的個人資料處理指南」主要是對事業，可以於開發商品前階段申請進行事前審查，與 PIPC 事先交流評估有無個資風險或違法情形。此一事前審查並非義務性要求，若有做此一事前審查，後續發生問題可以有罰鍰上的減免以為鼓勵。

13.匿假名資料

(1) PIPC 設有「假名資訊利用區域支援中心」及「假名資訊支援平台（https://dataprivacy.go.kr）」，提供假名處理基礎設施、假名處理方案、技術支援、假名處理適當性的審查與諮詢等服務。

(2) 南韓針對假名資料有特別規定，個資法此處指的是統計分析、公益性資料保存、科學技術發展研究(此部分包括民間產業之科學技術發展研究)才適用假名資料，商業用途則需要經過當事人同意。

(3) 目前有公布假名資料處理的指引，有非常詳細之資訊可供參考，包括假名處理諮詢、如何進行假名處理，以及假名處理的適當性。PIPC 並有聘僱假名處理專家，目前已經第二期評估，有 200 名專家協助假名資訊提供平臺之運作。

(4) 因假名資料結合很容易再識別，故必須由特定機關才可以進行假名資料結合。假名資料結合只要透過指定機關進行即可，無須經過委員會。指定機關不只委員會可指定，其他公務機關也可以指定，因為假名資料涉及領域多元，例如金融資料，就是金融主管機關指定，醫療資料則為醫療主管機關指定，當然 PIPC 亦可進行指定。而申請人限於資料主體。

■ PIDMC 組織及業務運作實務

1. PIDMC 之組成及與 PIPC 之關聯

PIDMC 與 PIPC 為二個獨立機關。PIDMC 之組成包含 1 位主任委員（委員長）共計 30 名委員，組成包括教授、律師、或相關團體之主管級成員。

2. 個資侵案調解案件處理流程

大量個資侵害發生，若欲取得賠償，會提出紛爭調解申請，若不同當事人之申請案為同一事件所導致，PIDMC 會將之併案處理。處理個案爭議之委員依法負有保密義務，不得外流侵害者與受害者之相關資料，以及爭議之內容。

3. 個人資料紛爭調解常見態樣

個資爭議調解侵害類型，其中最為常見者，為「未經同意蒐集個人資料」，其他尚有「過度蒐集個人資料」、「目的外利用或自第三方獲取資料」、「資料期限屆滿或目的達成後未刪除資料」、「個資管理者之技術、管理或實體措施不足」、「涉及查詢、更正、刪除及停止處理相關事宜」、「未遵守當事人撤回同意之要求」及其他涉及隱私侵害之行為等。

4. 紛爭調解成功率及對訴訟發生率之實益

紛爭調解委員會調解結果等同於司法調解之效果，可作為強

制執行之執行名義，與民事訴訟終局判決具有同等效力，原則上不得再提起訴訟。至於是否有效降低訴訟發生，PIDMC僅能統計所處理之調解案件，欠缺法院端之相關資料，故無法確定此程序確實降低訴訟發生率。但若當事人申請調解同時又去提起民事訴訟，則調解程序即會中止。

5. 紛爭調解案件之申請

當事人若向 KISA 或 PIPC 舉報個資侵害事件並決定進行民事求償，是否需另外提出紛爭調解申請，或由受理舉報機關直接轉達一節，PIDMC 表示，紛爭調解案件須另外申請，不得由受理侵害舉報之機關或機構直接轉達。

圖表 貳-6 考察團成員與 PIPC 國際合作擔當官合影

參、參訪心得與建議

本次考察之受訪單位於南韓個人資料保護獨立機關運作、組織、法制建構與執法層面皆有代表性，包括個資保護獨立監督機關（PIPC）、獨立之紛爭解決機關（PIDMC）、配合個資法由總統令指定之專業機關（KISA）、個資法配套驗證機制之驗證機構（OPA），以及匯集南韓具備影響力之個資專業人才協會（KAPP），除初步進行意見交流外，並建立未來我國個人資料保護委員會聯繫網絡，訪談之收穫可做為我國規劃獨立機關及配套機制過程之經驗參考，分述如次：

一、個資保護之執法與實務能量建構於制度層面有併同考量必要

本次考察團隊於拜會過程當中，皆針對拜會單位與 PIPC 或彼此間於個資法執法或措施推動的關係，進行了解。其中從 KISA、OPA 與 PIPC 之訪談過程，可以充分感受到獨立機關執法調查所需之專業資源，除了獨立機關本身須有一定能量外，專業機構功能定位之良善規劃，以及專業人力之適時支持，於制度推動有其重要性。尤其 KISA 扮演的角色，從搭配 PIPC 之公權力執法，到協助標準訂與推動制度的落實、驗證機構之認證評估等事宜，同時也是南韓政府於推動個資保護及資訊安全機制間之橋梁，可謂具備極為關鍵之角色。

PIPC 與各專業機構之互動合作，可歸納如以下層面：

(一)執法層面

PIPC 為個資法主要執法之主體，除其本身培養之調查人員外，個資執法所涉技術層面，可請 KISA 予以支持。KISA 並藉由個資法賦予之地位，協助 PIPC 處理包括侵害通報事件處理，以及共同維持外洩通報運作等事宜。

(二)提升公務及非公務機關法遵能量層面

南韓亦搭配國家認可之標準制度運作作為配套，尤其在訪談 KISA 與 OPA 部分可知，KISA 亦同時為建立國家法制面認可之 ISMS 與 ISMS-P 之標準制定機關與認證機關，雖然目前

僅有 ISMS 透過法律規範要求特定事業有導入並驗證通過之義務。ISMS-P 尚未透過法律予以義務化，但於裁罰標準層面直接公告得減少 40%以內之罰鍰金額，就實務而言亦形成相當之鼓勵。促使南韓事業，願意投入心力與資源進行導入，從管理制度層面提升其內部個資保護之控管，降低違法行為發生之疑慮。

(三)法制規劃非僅偏重執法層面

本節亦包括提升組織內部管理之配套措施，並從效果面加以鏈結，鼓勵事業予以導入，兼顧執法與組織體質之提升，或許是可以讓個資保護整體政策落實更完整之作法。OPA 於訪談中亦曾說明，早期 ISMS 並未被法制化與義務化，事業組織導入之意願即相對低落，法制化與義務化後，導入與驗證家數有所提升。但其亦提醒，各國國情不同，南韓法制化與義務化有其背景因素，ISMS-P 是否法制化並義務化則仍在討論，主因在於會影響事業營運之成本，此一經驗亦可提供國內法制度建構之思考。

二、個資保護及執法專業人力之養成與來源之建構需有所考量

南韓於個人資料保護專業人員之養成與機制，大致可以區隔執法面之人才養成，以及促進組織內部法遵人才養成二層面。

(一)PIPC 等執法層面之人才養成

目前已知 PIPC 本身仍是以取得公務員資格作為主要人才來源，但於特定領域需要得進行特別招聘或契約約聘。基本調查人員 30 名，就其所管轄之業務範圍而言，人數並不多。但其調查人員並可依據個案，於涉及技術層面依法要求 KISA 支援，對於調查人力與專業程度已有適度之補充。故對於獨立機關執法之專業人力來源，於制度規劃層面宜考量獨立機關本身來源可能性以及輔助單位協助之可能性。且從後續 PIPC 提供之教育訓練規劃，可知無論是對於新進調查人員以及對原調查人員之持續訓練規劃皆有其必要性。包括支持取得外部認證資格，或規劃對於新領域知識之養成，以

因應社會、經濟與技術環境之變化等，皆有其必要性。

(二)促進組織內部法遵人才養成

KISA 於本節扮演重要角色，透過政府預算之挹注，除協助普遍性個資保護意識提升外，並有對於實務個資專業人員層面，搭配個資法關於 CPO 設置之要求，進行人才儲備之訓練。同時也透過大學課程之規劃，由學校開始逐步豐富相關人才之培育。可以看出對於從事業組織內部法遵人才養成之重視。此處不僅是法律面對於強制 CPO 設置要求之必要搭配，同時亦可對應其於事業組織內部制度標準建構、權責人員設置與人才培育機制層面皆須有所搭配。再對應本次於 KAPP 訪談過程提及依法成立設置之 K-CPO 聯席會，亦是透過法律之鼓勵，使得事業個資專業管理人員得以相互聯繫學習，亦形成與 PIPC 間得以充分聯繫溝通之機制，可看出南韓個資監管體系對於專才養成並促使其於個資保護法遵執法能力與效能提升之整體思考。

三、對公務機關之監督以尊重自律為原則，輔以明確之審核與類似競賽之制度有其特色

有關 PIPC 如何落實個資法對於公務機關之監督，PIPC 釐清了個資法中對於個資保護基本計畫以及機關實施計畫之關係。因此體制上 PIPC 僅針對中央機關提出基本計畫，再由各中央機關自主建立實施計畫，交委員會審議與監督執行情形。於地方政府 PIPC 則尊重地方自治以及權責劃分，原則並不介入，並由行政安全部之實施計畫進行落實。故實際上對於公務機關之監督，PIPC 僅是於必要原則之把關，實際上仍尊重其他機關之權責以及自律。

特別的是，對於公部門之個人資料管理水準的診斷，反而是對其他公務機關壓力最大的部分，因依據審查診斷之結果會進行上中下分級，並會依據機關是否發生外洩及外洩情形給予年終成績加減分，最終會公布分類結果。同時搭配公務機關個資保護之風險評估機制，針對相關政策作為可能影響之個人資料情

況進行評價，分為 ABCD 等級，其結果亦會納入年度考核績效，最終並會公布結果。上述機制實施下來，雖然相關分數與評估結果，並不會影響受評估機關之預算，但機關會基於形象考量，提升度於個資保護之重視，可以說是有對應其國家機關特性之監督機制。足見監管機制之建構與可能的效果，應考慮國情特性加以設計，方能收其效能。

四、廣泛性之個人資料保護與特別法義務之關聯有思考空間，尚待進一步了解

本次考察其中一個諮詢重點，在於 PIPC 執法與其他機關構之間的關聯性，以及執法過程其他機關/構之角色以及是否可能獲取相當之支援。然而考察過程，對於機關之協助，PIPC 表示，基於個資法已明定部會協助之義務，故 PIPC 若提出協助之需要，基本上部會皆會進行協助。外洩調查部分若機關不提供協助，甚至有罰鍰之設計，故對於調查協助部分認為並無太大障礙。

然而，對於金融相關資料之外洩部分，於 KISA 之訪談中可以發現，實際上與個資法規範之個資外洩通報有所區隔，此部分應是涉及特別法關於信用資料之通報規定，針對銀行、保險公司、證券公司等金融機構之信用資料外洩，通報對象為金融委員會。而若非上述金融機構，而是一般交易行為導致之信用資料外洩，則回歸個資法之通報機制。此部分於個資法並未有對應之規範，而係因特別法對於特定機構與資料類型之特別規定。故南韓雖然並未如同日本，於個資法規範權限委任規定並由個資委列表進行權限委任，其仍有部分組織涉及之個人資料類型，係透過特別法之規定，由其他監督機關進行規制。

然而此部分僅是從訪談過程獲得資訊進行推測，是否除金融機構之信用資料層面有特別之作法，或有其他領域亦有相當之特別規定，尚待進一步了解。