案號：ndc106020

國家發展委員會 106 年度
「個人資料保護專責機關與資料在地化之法制研究」
委託研究計畫
結案報告

執行單位：達文西個資暨高科技法律事務所

研究主持人：葉奇鑫律師

研究員：王慕民律師、吳彥欽律師、陳品安律師

研究助理：廖又萱

中華民國 107 年 05 月 15 日

（本報告內容純係研究小組之觀點，不應引申為國家發展委員會之意見）

摘要

近年亞太地區陸續參照歐盟個資保護法制，推動個資法修法、設置個資保護專責機關並調整個資在地化相關規範，本研究即以歐盟、英國、加拿大、亞太地區（香港、澳門、日本、南韓、新加坡、馬來西亞、菲律賓、紐西蘭、澳洲)及國際組織(ICDPPC、APEC 之 CBPRs）等數個研究對象作為比較標的，分析各個研究對象對於個資保護專責機關之概述、法律依據、組織架構、法定職權，以及資料在地化規範等，以作為研析我國設置個資保護專責機關之可能立法模式及其利弊、所需配套、法規調適建議，以及個資保護專責機關於個資跨境傳輸所扮演之角色、功能與法規調適建議。

本研究聚焦於「個資與隱私保護專責機關」與「個人資料跨境傳輸與資料在地化」的國際實踐，於比較國際法例、規範後產出研究發現，並依此提出我國的修法建議。在「個資與隱私保護專責機關」部分，本研究於第二章綜整各研究對象對於個資與隱私保護專責機關的組織要求（專責性與獨立性）與法定職務等，提出我國如成立個資保護專責機關應具備之要件，並分析我國目前成立個資保護專責機關之可行性與法規調適建議。

在「個人資料跨境傳輸與資料在地化」方面，本研究於第三章整理各研究對象對於個人資料的跨境傳輸與資料在地化規範，認為我國應維持「有條件的跨境傳輸」立法模式。本研究建議，如配合個人資料保護委員會之成立，我國關於「國際傳輸個人資料」之規範即可改為「許可／同意，例外允許制」；若我國未能成立個資保護專責機關，則仍應維持現行「例外限制禁止制」，但對於中央目的事業主管機關在「審酌個人資料接受國對於個資保護是否具備完善之法規」時，應有法定標準以憑依據。

關鍵字：個資與隱私保護、專責機關、跨境傳輸、資料在地化

Summary

In recent years, several countries in the Asia Pacific region have begun to amend personal data legislations, establish specialized personal data protection agencies, and adjust data localization regulations, referencing the EU's personal data protection regime. Comparing EU, UK, Canada, Asia Pacific countries (Hong Kong, Macau, Japan, South Korea, Singapore, Malaysia, the Philippines, New Zealand, Australia) and international organizations (ICDPPC and CBPRs under APEC), this study provides overviews and analyses of the subjects' respective personal data regimes as well as their mandates, organizational structures, functions and data localization regulations. From these, this study then formulates suggestions on Taiwan's potential legislative models in establishing a specialized personal data protection agency, along with advantages, drawbacks, required corresponding measures and legislative adjustment suggestions. Suggestions on the role and functions of, and legislative adjustments for, this specialized agency is also provided in relations to cross-border transmission of personal data.

The focus of this study is the international practice on specialized personal data and privacy protection agencies and cross-border transmission and localization of personal data. By comparing international legal precedents and legislations, this study presents its findings, from which stem suggested amendments of Taiwan's law. On specialized personal data and privacy protection bodies, Chapter 2 presents the subjects' organizational requirements (specialization and independence) for, and mandated functions of, their respective specialized agencies, and provides suggestions on the conditions required

for Taiwan's establishment of a specialized agency of its own, as well as analyses on the legal feasibility and suggested required legislative adjustments for such an establishment.

On cross-border transmission and localization of personal data, Chapter 3 presents the subjects' respective regimes on cross-border transmission and localization of personal data and argues that Taiwan should maintain the current legislative model of "conditional cross-border transmission". This study suggests that, if Taiwan is to establish a Personal Data Protection Commission, it may change its model to "approve/consent by application with permissions given on exceptions" in terms of international transmission of personal data; if Taiwan is not able to establish a specialized personal data protection agency, it should maintain its current "restrict and prohibit on exceptions" model, with institutionalized criteria with which central agencies responsible for individual industries may determine the adequacy of the recipient country's personal data protection regime.

Keywords: Personal Data and Privacy Protection, Specialized Agency, Cross-border Transmission, Data Localization

目錄

表目錄

圖目錄

第一章 前言

第一節　研究目的

依據我國「《個人資料保護法》（以下簡稱個資法）」規定，法務部為個資法的法制主管機關，有權對個資法做出解釋，但個資法上的限制國際傳輸權（個資法第 21 條）、行政檢查權（個資法第 22 條）、指定安全維護權（個資法第 27 條第 2 項）、行政處罰權（個資法第 25 條、第 47 條至第 50 條）等，則劃歸各中央目的事業主管機關或直轄市、縣（市）政府之權責範圍。

此立法目的或為減輕法務部負擔，並尊重各中央目的事業主管機關或直轄市、縣（市）政府對所轄事業的監管權限，立意良善，然而，由各中央目的事業主管機關或直轄市、縣（市）政府自行決定是否及如何對所轄事業執行行政檢查、限制國際傳輸個人資料、行政處罰等，恐將造成「相同事件因主管機關不同而有寬嚴不一標準」之矛盾。

以本研究案之主題「資料在地化（跨境傳輸個人資料[1]）」為例，由個資法第 21 條規定「非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：一、涉及國家重大利益。二、國際條約或協定有特別規定。三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。四、以迂迴方法向第三國（地區）傳輸個人資料規避本法。」可知，現階段我國對於個人資料的跨境傳輸是採原則允許，例外得由中央目的事業主管機關予以限制的立法模式。

如上所述，法務部為個資法的解釋機關，但對於跨境傳輸的限制

[1] 雖個資法中稱為「國際傳輸」，但為配合　貴會委託研究用語，本研究將以「跨境傳輸」稱之。

與否又於個資法第 21 條規範中交由各中央目的事業主管機關自行判斷。姑不論各中央目的事業主管機關對於個資法的理解與掌握是否足夠針對所轄事業的特性制定跨境傳輸個人資料的限制標準，更何況在未有統一或建議標準的情況下，由於各中央目的事業主管機關對於個人資料保護法規的認知差異，難免造成各事業的管制落差，例如國家通訊傳播委員會曾以「個人資料保護法令尚未完備」為由，禁止所轄通訊傳播事業經營者將用戶個人資料傳輸至中國地區[2]，但同樣就企業將消費者個人資料傳輸至「個人資料保護法規不足」之中國一事，其他中央目的事業主管機關對所轄事業卻無任何禁止或限制，實難有合理理由解釋此間之矛盾。

且就「資料在地化（跨境傳輸個人資料）」而言，為保護國民個人資料的安全並兼顧個人資料的流通，如何確保國民的個人資料在傳輸至第三國（地）後不致遭到濫用、誤用或洩漏等侵害，主管機關責無旁貸。然而如前所述，我國對於個人資料的跨境傳輸規範於個資法第 21 條，該規範僅列出中央目的事業主管機關得限制傳輸的消極條件，乃「例外限制」之立法模式，此與國際上多數國家之採「例外允許」之規範大相逕庭，是否對於我國國民的資訊隱私權、自主權等憲法上權利保障有所不足，亦值得比較探討。

有鑑於此，本研究即以歐盟、英國、加拿大、亞太地區等國為研究對象，分析各國設置個資與隱私保護專責機關之組織規範及法定職務，並研究各國對於個人資料跨境傳輸的規範強度，以此通盤檢討並採納適合我國的調整措施，以期達到強化國民個資保護並平衡兼顧個人資料流通的合理使用目的。

---

[2] 國家通訊傳播委員會 101 年 9 月 25 日通傳通訊字第 10141050780 號令參照。

第二節　研究方法

一、文獻分析法

為研究我國設立專責機關之可行性及面臨之相關法律議題，本研究案擬藉由既有碩博士論文、期刊論文、研究報告、考察報告及實務上法令、行政函釋及法院判決等文獻作為研究的基礎及對象，除剖析我國個人資料保護之權責與裁罰係分散於各中央目的事業主管機關及直轄市、縣（市）政府，法務部則為個資法解釋機關之外，再參考其他國家之實務案例、法制規範、管制經驗與發展趨勢，進一步針對個資保護專責機關設置及個資在地化之法制架構進行相關研析。

二、比較法研究

由於我國目前尚未設立個資保護專責機關，為瞭解國際上對於個資法專責機關設置與資料在地化等規範之趨勢，因應我國個資保護發展現況，本研究擬以比較法研究方式，考量代表性、參考性、實用性及語言便利性，挑選**歐盟**（全球個資與隱私保護的指標，最新個資保護法律《General Data Protection Regulation, GDPR》將於 2018 年 5 月 25 日生效）、**英國**（即將於 2019 年 3 月 30 日脫離歐盟的個資保護先進國家）、**加拿大**（經歐盟認定具備個資保護適足性而可跨境傳輸個資之國家）、**澳紐**（南半球的個資保護先進國家）、**亞太國家**（臨近台灣而足作為借鏡比較之**港、澳、日、韓、新、馬、菲**）、**國際組織**（我國可爭取參加的「**個資與隱私保護委員國際研討會 ICDPPC**」及「**APEC 跨境個資保護規則體系 CBPRs**」）等數個研究對象作為比較標的。

本研究將比較並彙整上述研究對象對於個資保護專責機關之概述、法律依據、組織架構、法定職權，以及資料在地化規範等，以作為研析我國如設置個資保護專責機關之利弊及可能立法模式、所需配套、法規調適建議，以及個資保護專責機關於個資跨境傳輸所扮演之角色、功能與法規調適建議。

第二章 個資與隱私保護專責機關

第一節 歐盟

一、概述

個資保護監督機關在歐盟具有憲法上的地位，依《歐盟運作條約（The Treaty On The Functioning of The European Union）》第16條第2項[3]及歐盟《基本權利憲章（Charter of Fundamental Rights of the European Union）》第8條第3項規定[4]，歐盟會員國應有獨立監督機關來監管個資保護相關規定的遵循；且歐洲法院曾於判決中認為，各會員國的個資保護監督機關乃人民基本權利與自由的守護者（guardians），其存在係對當事人在個資處理行為中提供保護的不可或缺之元素（essential component）[5]，並能「建立隱私生活權利保障及個人資料自由流通兩者之平衡」[6]。

二、法律依據

歐盟於1995年制定《個人資料保護指令（95/46/EC）》，20年過去，由於科技發展的迅速，資料控制者（Controller）對於

---

[3] EU, the Treaty on the Functioning of the European Union, Article16.2, "The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities".

[4] EU, Charter of Fundamental Rights of the European Union Article8.3, "Compliance with these rules shall be subject to control by an independent authority".

[5] European Court of Justice, Case C-518/07, *Commission v Germany*, 2010, para23, "The supervisory authorities provided for in Article 28 of Directive 95/46 are therefore the guardians of those fundamental rights and freedoms, and their existence in the Member States is considered, as is stated in the 62nd recital in the preamble to Directive 95/46, as an essential component of the protection of individuals with regard to the processing of personal data".

[6] European Court of Justice, Case C-518/07, *Commission v Germany*, 2010, para30, "…their task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data".

當事人（Data Subject）個人資料的蒐集、處理與利用的廣度與深度已非 1995 年制定的指令所能涵蓋，且當事人的權利亦隨著資料控制者的強勢而更顯不足，有鑒於此，為消弭資料控制者與當事人間的權責失衡，並對受資料控制者委託的資料處理者（Processer）亦加諸受規管之責，同時就歐盟境內會員國的適用法律與監管方式給予一致性的規範，歐盟遂於 2012 年提出歐盟《個資保護規則（General Data Protection Regulation）》草案，並在 2016 年 5 月公布正式條文，施行日期則為 2018 年 5 月 25 日，將於歐盟各會員國內直接生效。

而有關個資與隱私保護監督機關的相關規定在《個人資料保護指令》時期即有規範，現則訂定於《個資保護規則》第 6 章中，詳見下述。

三、監督機關及其獨立性

(一) 設置獨立監督機關

依《個資保護規則》規定，各會員國應設立一個以上的獨立監督機關以負責監管《個資保護規則》的落實，以此保障處理個資及促進個資流動時的資料當事人基本權利與自由[7]。而各個監督機關均應促成《個資保護規則》在歐盟境內適用的一致性，因此，各個監督機關應依《個資保護規則》第 7 章規定互相協助，並與執委會合作[8]。

---

[7] EU, GDPR, Article51.1, "Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (‘supervisory authority’)".

[8] EU, GDPR, Article51.2, "Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate

又如一會員國設有複數監督機關時,應指派其一作為對歐盟個資保護委員會（European Data Protection Board）的代表,並建立確保其他監督機關均能遵循《個資保護規則》第 63 條有關「規則適用一致性機制(consistency mechanism)」的體系[9]。

(二) 監督機關之獨立性

各監督機關在執行《個資保護規則》所定任務及行使職權時,應享有完全之獨立性[10]。其成員在依《個資保護規則》執行其任務及行使職權時，應保有不受外來直接或間接影響的自主性，並不得接受或尋求任何人的指示[11]，且無論有無酬勞，成員應避免任何與其任務相悖之行為，並不得於在職時擔任任何與其任務相悖之職位[12]。

各會員國應確保提供各監督機關必要的人力、技術、經費、場所、設施，以供其有效執行法定職務及行使職權，包含互助、合作及參與歐盟個資保護委員會[13]，並應確保各

---

with each other and the Commission in accordance with Chapter VII".

[9] EU, GDPR, Article51.3, "Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63".

[10] EU, GDPR, Article52.1, "Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation".

[11] EU, GDPR, Article52.2, "The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody".

[12] EU, GDPR, Article52.3, "Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not".

[13] EU, GDPR, Article52.4, "Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board".

監督機關享有機關的人事決定權[14]。

此外，各會員國應確保各監督機關的財務控管不致影響其獨立性，並享有可包含於整體國家預算中的專屬公務年度預算[15]。

(三) 歐盟實務對監督機關獨立性之判斷

無論依《個人資料保護指令》或《個資保護規則》，歐盟會員國成立的個資保護監督機關均應具備「完全之獨立性（complete independence）」，此「獨立性」要件在歐盟實務上不乏爭議，以下即對「歐盟判斷境外國家是否具備個資保護適足性而得將境內當事人個資跨境傳輸至該境外國家時，對該境外國家的個資保護監督機關之獨立性審查」及「歐洲法院對歐盟會員國個資保護監督機關的獨立性審查」兩部份分述之。

1、適足性審查案例

由於「境外國家或地區具備個資保護適足性（adequacy）」係歐盟允許無須批准即可跨境傳輸境內當事人個資至該境外國家或地區的要件(詳見第三章)，因此歐盟執委會需對該境外國家詳為審查，以確定是否具備個資保護適足性。

---

[14] EU, GDPR, Article52.5, "Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned".

[15] EU, GDPR, Article52.6, "Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget".

執委會現行的審查基準仍係按照 1998 年公布的工作文件所示[16]，指標略為：「該境外國家或地區之個資或隱私保護法律是否具備歐盟法規的重要原則」，例如目的限制、必要範圍、資料品質、透明性、安全維護、當事人權利等，以及「該境外國家或地區的法律體系是否對前述法規具備足夠的執行機制」，例如「能否實現良好法律遵循」、「能否有效支援當事人行使權利」及「是否對被害人有適當補償」。

其中對於「能否實現良好法律遵循」的審查依據包含「個資保護監督機關之存在」和「該機關的執法能力與裁罰能力」，而在審查「監督機關的存在及能力」時，執委會即會考量該監督機關是否具備「完全的獨立性」。

以截至本研究報告交付日已通過歐盟「適足性審查」的國家為例（美國除外，因美國係以「企業符合歐美 Privacy Shield 隱私保護標準」之方式判斷個別企業之適足性標準，並非以「美國之個資保護法規是否符合歐盟適足性要件」予以認定）[17]，依歐盟公布之相關文件提及者，約可將歐盟對於「監督機關獨立性」的判斷參考依據整理如下：

（1）法律賦予監督機關（首長）之組織獨立性或獨立行

[16]《Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive》, WP12, 1998.

[17] 阿根廷、根西（Guernsey）、曼島（Isle of Man）、瑞士、加拿大、澤西（Jersey）、法羅群島（Faroe Islands）、安道爾（Andorra）、以色列、烏拉圭、紐西蘭。

使職權之權利

例如阿根廷[18]、根西[19]、澤西[20]、法羅群島[21]、瑞士[22]、加拿大[23]、安道爾[24]、烏拉圭[25]及紐西蘭[26]。

（2）監督機關首長／成員之任免保障

---

[18] 《Opinion 4/2002 on the level of protection of personal data in Argentina》,WP63, 2002, p14, "The Director shall exercise his functions with full independence and he shall not be subject to instructions".

[19] 《Opinion 5/2003 on the level of protection of personal data in Guernsey》，WP79, 2003, p8, "The Commissioner is fully independent, as stated in Article 6.4 of the Law: *The Commissioner is not a servant or agent of the States, but is a holder of public office and is under a duty to discharge the functions of that office with complete fairness impartiality and independence*".

[20] 《Opinion 8/2007 on the level of protection of personal data in Jersey》, WP141, 2007, p10, "It has the legal status of a 'corporation sole', making it an agency which is both independent of government and possesses a legal status which will continue in the event of the person holding the office ceasing to do so".

[21] 《Opinion 9/2007 on the level of protection of personal data in the Faroe Islands》, WP142, 2007, p10, "The Data Protection Agency, consisting of a Board and a Secretariat, is responsible for the supervision of all processing operations covered by this Act, and shall act with complete independence in executing the functions entrusted to it".

[22] 《The application of Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland》, 2004, p5, "The SFADP also provides for appropriate institutional mechanisms, such as an independent supervisory authority with appropriate powers".

[23] 《The application of Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documentation Act》, 2006, p6, "Canadian legislation provides for appropriate institutional mechanisms, such as an independent supervisory authority with appropriate powers and appropriate recourse before the courts in case of violations of privacy. The Privacy Commissioner of Canada acts as an independent ombudsman and reports directly to the Parliament, not to the government in power".

[24] 《Opinion 7/2009 on the level of protection of personal data in the Principality of Andorra》, WP166, 2009, p11, "an independent authority that acts with objectivity and full independence of the Andorran public administrations in the exercise of its functions and is related to the Government via the Ministry responsible for the Economy".

[25] 《Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay》, WP177, 2010, p15-16, "The LPDP, by virtue of Article 31, created the control authority for data protection, called the "Unit for the Regulation and Control of Personal Data" (URCDP in Spanish) which is an "autonomous entity of the Agency for the Development of Electronic Government and the Knowledge-Based Society (AGESIC in Spanish)…the LPDP expressly states that the members of the Executive Council "shall not receive orders nor instructions on technical matters"".

[26] 《Opinion 11/2011 on the level of protection of personal data in New Zealand》, WP182, 2011, p13, "Section 13(1A) of the Privacy Act provides that the Commissioner must act independently in performing his or her statutory functions and duties and in exercising his or her statutory powers".

A. 阿根廷

雖然阿根廷個資法律賦予個資保護監督機關「國家個資保護理事會（National Directorate for the Protection of Personal Data, DNPDP）」首長獨立行使職權之權，但由於該機關「於組織上隸屬於法務與人權部（Ministry of Justice and Human Rights）」，其首長係「由部長提名」，且「得由部長予以免職」，又該機關之人員配置「均由部長決定」，**歐盟遂對該機關是否享有「完全之獨立性」存有疑慮**[27]，並呼籲阿根廷應在法制上有對應之調整。

B. 澤西

澤西「個資保護委員（Data Protection Commissioner[28]）」由議會選出，且於任期內僅得由議會終止任期[29]。

C. 法羅群島

法羅群島個資保護監督機關「個資保護局（Data Protection Agency）」的委員會委員雖由

---

[27] 《Opinion 4/2002 on the level of protection of personal data in Argentina》,WP63, 2002, p14, "The Working Party considers that this situation does not guarantee that the authority may act in complete independence".

[28] Commissioner 一詞於我國未有統一翻譯，其內涵依各國法制可為「合議制之委員（長）」或「首長制之機關首長」。本研究為行文統一，以「委員」稱之。

[29] 《Opinion 8/2007 on the level of protection of personal data in Jersey》, WP141, 2007, p10, "Insofar as the Commissioner is appointed by the States, which is the parliament, and can only be dismissed by the States there is no doubt on the ability of the Commissioner to perform her duties in complete independence".

法務部長（Minister of Justice）指派，但享有 4 年的任期保障[30]。

D. 以色列

以色列個資保護監督機關「法律、資訊與科技管理局（The Israeli Law, Information and Technology Authority, ILITA）首長的任期僅得在特定條件下經「由前任法官領導的特別公務員委員會」決議終止，且得對該決議提出司法審查[31]。

E. 安道爾

安道爾個資保護監督機關「個資保護局（Andorran Data Protection Agency, APDA）」首長的任免均由安道爾的立法機關「總委員會（Consell General）」決定[32]。

F. 烏拉圭

烏拉圭個資保護監督機關「個資監管組

[30]《Opinion 9/2007 on the level of protection of personal data in the Faroe Islands》, WP142, 2007, p10, "The members of the Board are appointed by the Minister of Justice for a term of 4 years. As a general rule, the members of the Board cannot be dismissed".

[31]《Opinion 6/2009 on the level of protection of personal data in Israel》, WP165, 2009, p15, "The functions of Head of ILITA may be terminated only in special circumstances by a special Civil Service Commission committee headed by a former judge……any decision to terminate the Head of ILITA would be subject to judicial review in which reasonable grounds would have to be shown".

[32]《Opinion 7/2009 on the level of protection of personal data in the Principality of Andorra》, WP166, 2009, p11, "the rules contained in the LQPDP and in the Regulations of the APDA show the independence of the latter both with regard to the appointment and dismissal of its Director and the two Inspectors that comprise it and with regard to its budgetary independence, given that both the appointment and dismissal of the said persons and the budget of the Agency are approved by the legislative Power (Consell General), requiring in the first two cases a specially qualified majority".

（The Unit for the Regulation and Control of Personal Data, URCDP）隸屬於「電子化政府與知識社會發展局（Agency for the Development of Electronic Government and the Knowledge-Based Society, AGESIC），其執行委員會（Executive Council）由一位 AGESIC 的執行主管及兩位經總統任命的委員組成，後兩位委員享有 4 年的任期保障[33]。

雖然個資監管組的執行主管隸屬 AGESIC，但歐盟審查後認為烏拉圭法律特別強化兩位由總統任命的委員於執行議會中的功能，並減弱執行主管的權力，可視為以此保證該個資監管組的獨立性[34]。

又歐盟認為，烏拉圭於 2009 年政權移轉後，該個資監管組並無任何異動，此亦為肯定該監管機關具備足夠獨立性之判斷依據[35]。

（3）監督機關之決定（處分）僅能由司法審查推翻

---

[33] 《Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay》, WP177, 2010, p16, "Except for the Executive Director of AGESIC, members shall remain in office for four years".

[34] 《Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay》, WP177, 2010, p16, "the regulation established in the DPDP strengthens the role of the two members of the Executive Council other than the Executive Director of AGESIC, with the latter's role being reduced and guaranteeing greater independence for the control body".

[35] 《Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay》, WP177, 2010, p16, "the Working Party accepts that the independence of the control body has been shown in practice as there has been no alteration whatsoever in its activity as a consequence of the change of government that took place in Uruguay in 2009".

A. 阿根廷

對阿根廷國家個資保護理事會首長之決定不服者，應依行政程序向法院提起救濟[36]。

B. 安道爾

對安道爾個資保護局之決定不服者，僅得逕向法院提起救濟[37]。

（4）監督機關有獨立預算或其他財務來源

A. 法羅群島

法羅群島個資保護局雖轄屬法務部，但依國會審查而具有獨立預算[38]。

B. 安道爾

安道爾個資保護局依法由立法機構「總委員會」決定其獨立預算[39]。

C. 以色列

---

[36] 《Opinion 4/2002 on the level of protection of personal data in Argentina》,WP63, 2002, p14, "His decisions can be appealed through the courts, according to the general rules on administrative procedures".

[37] 《Opinion 7/2009 on the level of protection of personal data in the Principality of Andorra》, WP166, 2009, p11, "it takes into consideration in order to appreciate this independence that the resolutions of the APDA may only be appealed against before the courts".

[38] 《Opinion 9/2007 on the level of protection of personal data in the Faroe Islands》, WP142, 2007, p10, "The DPA is funded from the Faroese budget, which is decided by the Faroese Parliament. The DPA is attached to the budget which is allowed by the Parliament to the Minister of Justice".

[39] 《Opinion 7/2009 on the level of protection of personal data in the Principality of Andorra》, WP166, 2009, p11, "the rules contained in the LQPDP and in the Regulations of the APDA show the independence of the latter both with regard to the appointment and dismissal of its Director and the two Inspectors that comprise it and with regard to its budgetary independence, given that both the appointment and dismissal of the said persons and the budget of the Agency are approved by the legislative Power (Consell General), requiring in the first two cases a specially qualified majority".

依照以色列法律規定，法律、資訊與科技管理局收取之資料庫註冊費將納入基金，並歸屬於該局供執行其任務[40]。

2、司法審查案例

除上述行政審查案例外，歐洲法院近年亦有幾則針對歐盟會員國個資保護監管機關之「獨立性」標準的司法判決可供借鏡，雖然下列判決均以現行歐盟《個人資料保護指令》作為法律依據，但由於《個人資料保護指令》第 28 條第 1 項與 GDPR 第 52 條第 1 項對監管機關要求的「獨立性」規範文字完全相同（shall act with complete independence），應可推論這些判決見解在 GDPR 生效後仍能適用，分述如下。

（1）Case C-518/07, Commission v. Germany, 2010

本案背景為歐盟執委會認為德國「**要求各邦個資保護監督機關統一受國家政府監管**」一事牴觸《個人資料保護指令》第 28 條第 1 項對於各會員國個資保護監督機關須有「完全之獨立性」的要求，因此請求歐洲法院宣告德國政府違背法律義務。

歐盟執委會主張，條文中所謂「完全之獨立

[40] 《Opinion 6/2009 on the level of protection of personal data in Israel》, WP165, 2009, p15, "……the funds resulting from the collection of fees for the registration of databases directly revert to ILITA as the supervisory authority for the development of the functions which have been attributed to it by Law".

性（complete independence）必須解釋為「**監督機關應不受任何影響，無論該影響來自政府內外**」[41]。而德國政府要求各邦個資保護監督機關統一受國家監管，係違反該條文之行為。

德國政府則抗辯，條文要求個資保護監督機關具備之獨立性係指該機關不應受到任何來自外在之影響，然而，「**國家行政監管行為（State scrutiny）並不構成來自外在之影響**」，而是德國行政體制下的「**內部監督機制**」[42]。

對此，**歐洲法院**於審理後提出下列說明並作出判斷：

A. 解釋《個人資料保護指令》條文時，須同時考量文義解釋、目的解釋及體系解釋[43]。

B. 以文義解釋來看，對公務機關而言，「獨立性」一詞通常應理解為「**可自由行使職權，無須接受任何指示或面對任何壓力**」[44]。

---

[41] European Court of Justice, Case C-518/07, *Commission v. Germany*, 2010, para15, "…'with complete independence' must be interpreted as meaning that a supervising authority must be free from any influence, whether that influence is exercised by other authorities or outside the administration".

[42] European Court of Justice, Case C-518/07, *Commission v. Germany*, 2010, para16, "…the State scrutiny exercised in the German *Länder* does not constitute such an external influence, but rather the administration's internal monitoring mechanism".

[43] European Court of Justice, Case C-518/07, *Commission v. Germany*, 2010, para17, "…the wording itself of that provision and the aims and scheme of Directive 95/46 should be taken into account".

[44] European Court of Justice, Case C-518/07, *Commission v. Germany*, 2010, para18, "In relation to a public body, the term 'independence' normally means a status which ensures that the body concerned can act completely freely, without taking any instructions or being put under any pressure".

C. 同時，條文中既強調「完全」之獨立性，即意旨「**該監督機關在做出任何決定時，均得享有不受任何直接或間接來自外部之影響的獨立性**」[45]。

D. 又從目的解釋以觀，《個人資料保護指令》對監督機關須有獨立性之要求，「**旨在確保監督機關行使職權的有效性及可靠性**」[46]，以此強化對於任何因監督機關之決定而受影響的自然人或監督對象的保障，意即監督機關在行使職權時必須客觀且公正[47]。為了達成此目的，監督機關不應受任何外在之影響，「**包含直接或間接來自國家中央政府或各邦政府的干預**」[48]。

E. 再從體系解釋觀之，規範歐盟各會員國的《個人資料保護指令》應與規範歐盟共同體機構的《個資保護規則 Regulation No 45/2001》作相

---

[45] European Court of Justice, Case C-518/07, *Commission v. Germany*, 2010, para18, "…the concept of 'independence' is complemented by the adjective 'complete', which implies a decision-making power independent of any direct or indirect external influence on the supervisory authority".

[46] European Court of Justice, Case C-518/07, *Commission v. Germany*, 2010, para25, "The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the supervision of compliance with the provisions on protection of individuals with regard to the processing of personal data".

[47] European Court of Justice, Case C-518/07, *Commission v. Germany*, 2010, para25, "…in order to strengthen the protection of individuals and bodies affected by their decisions. It follows that, when carrying out their duties, the supervisory authorities must act objectively and impartially".

[48] European Court of Justice, Case C-518/07, *Commission v. Germany*, 2010, para25, "For that purpose, they must remain free from any external influence, including the direct or indirect influence of the State or the *Länder*".

同之解釋[49]，後者創設「European Data Protection Supervisor, EDPS」作為歐盟共同體層級的個資保護監督機關，並於第 44 條第 1 項規定 EDPS 在執行任務時應有完全之獨立性，第 2 項則補充前述獨立性之內涵包括「EDPS 在執行任務時無須尋求或接受任何人的指示」[50]。

F. 既然《個資保護規則 Regulation No 45/2001》第 44 條與《個人資料保護指令》第 28 條係源自同一觀念，兩者之解釋即應具備一致性，因此，各會員國個資保護監督機關之獨立性要求亦應包含「執行任務時無須接受任何指示」[51]。

G. 據此，《個人資料保護指令》第 28 條所稱「完全之獨立性」應解釋為「**個資保護監督機關於執行任務時，不僅不受監督對象的影響，更包含不受任何直接或間接之指示或來自外在之影響，以避免監督機關之行為遭到質疑（call**

[49] European Court of Justice, Case C-518/07, *Commission v. Germany*, 2010, para25, "…the scheme of Directive 95/46, the latter must be understood as the equivalent of Article 286 EC and Regulation No 45/2001".

[50] European Court of Justice, Case C-518/07, *Commission v. Germany*, 2010, para27, "In accordance with Article 44(1) of Regulation No 45/2001, that body is to perform its duties in complete independence. Article 44(2) thereof clarifies that concept of independence by adding that, in the performance of its duties, the EDPS may neither seek nor take instructions from anybody".

[51] European Court of Justice, Case C-518/07, *Commission v. Germany*, 2010, para28, "In view of the fact that Article 44 of Regulation No 45/2001 and Article 28 of Directive 95/46 are based on the same general concept, those two provisions should be interpreted homogeneously, so that not only the independence of the EDPS, but also that of the national authorities, involve the lack of any instructions relating to the performance of their duties".

into question）」[52]。

H. 在本案中，首應認清德國的「國家行政監管行為」無論採取何種形式，本質上即允許各邦政府或行政機關接受中央政府直接或間接影響其所作之決定，甚至撤銷或變更之[53]。

I. 即便德國政府宣稱該監管制度僅是為了確保各邦個資保護監督機關之行為遵循德國及歐盟法律規範，然而，執行監管之機關既隸屬國家行政體制而受各邦政府控管，便有可能無法客觀解釋及適用個資保護法律[54]。

J. 然而，此行政監管制度將使個資保護監督機關在作出決定時存有「**事前遵循（prior compliance）**」執行監管機關意旨的可能[55]，但

---

[52] European Court of Justice, Case C-518/07, *Commission v. Germany*, 2010, para30, "IIn the light of the foregoing, the second subparagraph of Article 28(1) of Directive 95/46 is to be interpreted as meaning that the supervisory authorities responsible for supervising the processing of personal data outside the public sector must enjoy an independence allowing them to perform their duties free from external influence. That independence precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task".

[53] European Court of Justice, Case C-518/07, *Commission v. Germany*, 2010, para32, "It should be noted that the State scrutiny, whatever form it takes, in principle allows the government of the respective *Land* or an administrative body subject to that government to influence, directly or indirectly, the decisions of the supervisory authorities or, as the case may be, to cancel and replace those decisions".

[54] European Court of Justice, Case C-518/07, *Commission v. Germany*, 2010, para34, "…the possibility remains that the scrutinising authorities, which are part of the general administration and therefore under the control of the government of their respective *Land*, are not able to act objectively when they interpret and apply the provisions relating to the processing of personal data".

[55] European Court of Justice, Case C-518/07, *Commission v. Germany*, 2010, para36, "…there could be 'prior compliance' on the part of those authorities in the light of the scrutinising authority's decision-making practice".

個資保護監督機關作為隱私生活權利的守護者，**其決定及機關本身均不得存有任何偏頗之虞**[56]。因此，即便只有極小風險（mere risk）會發生執行監管機關以政治力影響各邦個資保護監督機關作出之決定，也已足夠削減個資保護監督機關執行職務的獨立性[57]。

基於上述理由，**歐洲法院認為德國政府之行為侵害《個人資料保護指令》對會員國個資保護監督機關要求的「完全之獨立性」**。

（2）Case C-614/10, Commission v. Austria, 2012

本案背景為歐盟執委會認為，奧地利個資保護監督機關「個資保護委員會（DSK）」的**組織法律牴觸《個人資料保護指令》第 28 條第 1 項對於各會員國個資保護監督機關須有「完全之獨立性」的要求**，因此請求歐洲法院宣告奧地利政府違背法律義務。

歐盟執委會主張，首先，根據奧地利法律，DSK 的管理階層成員均為「聯邦總理府（Federal Chancellery）」的官員，因此 DSK 每日業務事實上

[56] European Court of Justice, Case C-518/07, *Commission v. Germany*, 2010, para36, "…it is necessary that their decisions, and therefore the authorities themselves, remain above any suspicion of partiality".

[57] European Court of Justice, Case C-518/07, *Commission v. Germany*, 2010, para36, "…the mere risk that the scrutinising authorities could exercise a political influence over the decisions of the supervisory authorities is enough to hinder the latter authorities' independent performance of their tasks".

均由受聯邦總理府指示、管轄的官員來管理[58]；其次，DSK 辦公室屬於聯邦總理府的部門，因此在組織上不具備足夠的獨立性，且 DSK 的所有成員均依法規受聯邦總理府管理監督[59]；最後，奧地利法律規定，聯邦總理府有權隨時接受 DSK 首長或管理階層成員對於任何業務執行的通知（the right to be informed）[60]。基於上述理由，奧地利的相關法律已抵觸《個人資料保護指令》要求個資保護監督機關須具備之「獨立性」。

奧地利政府則抗辯，《個人資料保護指令》第 28 條第 1 項所稱之「獨立性」係指「**功能上的獨立**」，而奧地利法律已規定 DSK 之成員應獨立行使職權而無須接受任何形式的指示[61]；而 DSK 得本於自主性，自行修改內部規則而自由決定指派

---

[58] European Court of Justice, Case C-614/10, *Commission v. Austria*, 2012, para25, "…the managing member of the DSK must always be an official of the Federal Chancellery. All day-to-day business of the DSK is thus de facto managed by a federal official, who remains bound by the instructions issued by his employer and is subject to supervision within the terms of Paragraph 45(1) of the BDG 1979".

[59] European Court of Justice, Case C-614/10, *Commission v. Austria*, 2012, para26, "…the DSK is structurally integrated with the departments of the Federal Chancellery. As a result of that integration, they contend, the DSK is not independent in either organic or substantive terms. All DSK staff members are, as is apparent from Paragraph 38(2) of the DSG 2000 and from Article 7(1) of the internal rules, under the authority of the Federal Chancellery and are thus subject to its supervision".

[60] European Court of Justice, Case C-614/10, *Commission v. Austria*, 2012, para13, "Paragraph 38(2) of the DSG 2000 provides: 'In support of the work of the [DSK], the Federal Chancellor shall establish an office and shall make available the necessary equipment and staff. The Federal Chancellor shall have the right to be informed at all times by the chairman and the managing member of all aspects of the work of the [DSK].'".

[61] European Court of Justice, Case C-614/10, *Commission v. Austria*, 2012, para30, "According to the Republic of Austria, the second subparagraph of Article 28(1) of Directive 95/46 relates to functional independence. The DSK has such independence since, in accordance with Paragraph 37(1) of the DSG 2000, its members are independent and are not bound by instructions of any kind in the performance of their duties".

管理階層成員[62]；且由奧地利預算法的角度來看，所有聯邦公務機關均隸屬於行政部門，此為奧地利政府與國會為確保所有行政機關均享有平等資源的共同決定[63]，況 DSK 的成員在組織上（包含職級及薪資等級）隸屬聯邦總理府亦不影響其獨立性[64]；最後，聯邦總理府的「受通知權」是為確保自主機關（autonomous bodies）與國會間的民主體制關係（democratic link），該權利並不使 DSK 的功能受到任何影響[65]。

對此，**歐洲法院**於審理後提出下列說明並作出判斷：

A. 功能上的獨立性尚不足使個資保護監督機關避免所有外部影響[66]。

B. 若 DSK 的管理階層成員均來自聯邦主管機關（聯邦總理府），依通常認知，兩者間將存有

---

[62] European Court of Justice, Case C-614/10, *Commission v. Austria*, 2012, para32, "…the DSK can itself freely decide whom to appoint as its managing member by amending, on an autonomous basis, its internal rules".

[63] European Court of Justice, Case C-614/10, *Commission v. Austria*, 2012, para33, "…all bodies of the federal public administration come, from the point of view of budgetary law, under a ministerial department. It is for the Government, in conjunction with the Parliament, to ensure that the various executive bodies have adequate equipment and staff".

[64] European Court of Justice, Case C-614/10, *Commission v. Austria*, 2012, para33, "…The fact that the staff of the office are, in legal terms, attached to the Federal Chancellery, both in terms of hierarchy and remuneration, does not affect their independence".

[65] European Court of Justice, Case C-614/10, *Commission v. Austria*, 2012, para34, "…as regards the 'right to information' of the Federal Chancellor, the Republic of Austria notes that that right seeks to ensure a certain democratic link between the autonomous bodies and the Parliament. The right to information provides no scope for the exercise of influence over the DSK's functioning".

[66] European Court of Justice, Case C-614/10, *Commission v. Austria*, 2012, para42, "…such functional independence is not by itself sufficient to protect that supervisory authority from all external influence".

隸屬關係的連結，而使管理階層成員的行為活動可受其主管的指示監督[67]。儘管奧地利法律規定 DSK 成員無須接受任何形式的指示，但該隸屬關係的事實仍使 DSK 管理階層成員的主管有權實施監督，因此削減 DSK 在執行職務上的獨立性[68]，並可能導致 DSK 管理階層成員「**事前遵循**」其主管的意旨[69]，也使 DSK 無法避免有偏頗之虞[70]。

C. 誠然，如同歐盟個資保護監督機關 EDPS 無須獨立於歐盟之外享有獨立預算（但歐盟應於預算中將 EDPS 的專屬預算單獨列出）[71]，DSK 不具獨立之預算亦不必然影響其獨立性[72]，然而，DSK 必要資源之來源不得使其在執行任務時無法具備完全之獨立性，但由於 DSK 仰賴其成員協助執行任務，而事實上其辦公室成員多係來自聯邦總理府之官員，此情況將使 DSK

---

[67] European Court of Justice, Case C-614/10, *Commission v. Austria*, 2012, para48, "…it is common ground that there is a service-related link between the managing member and that federal authority which allows the activities of the managing member to be supervised by his hierarchical superior".

[68] European Court of Justice, Case C-614/10, *Commission v. Austria*, 2012, para50, "…the fact remains that Paragraph 45(1) of the BDG 1979 confers on the hierarchical superior a power of supervision that is liable to hinder the DSK's operational independence".

[69] European Court of Justice, Case C-614/10, *Commission v. Austria*, 2012, para51, "…could lead to a form of 'prior compliance' on the part of the managing member".

[70] European Court of Justice, Case C-614/10, *Commission v. Austria*, 2012, para52, "…by reason of the links that the managing member of the DSK has with the political body, which is subject to the supervision of the DSK, the latter is not above all suspicion of partiality".

[71] EU, Regulation No 45/2001, Article43.3, "The European Data Protection Supervisor's budget shall be shown in a separate budget heading in Section VIII of the general budget of the European Union".

[72] European Court of Justice, Case C-614/10, *Commission v. Austria*, 2012, para58, "…the DSK need not be given a separate budget, such as that provided for in Article 43(3) in Regulation No 45/2001 for the EDPS, in order to be able to satisfy the criterion of independence".

的決定有遭受影響的風險[73]。

D. 最後，聯邦總理府依法享有「受通知權」，將導致 DSK 間接受到聯邦總理府的影響[74]，使 DSK 在執行任務時存有偏頗之虞[75]。

基於上述理由，**歐洲法院認為奧地利政府之行為侵害《個人資料保護指令》對會員國個資保護監督機關要求的「完全之獨立性」**。

（3）Case C-288/12, Commission v. Hungary, 2014

本案背景為匈牙利原於 2008 年依法指派一位個資保護監察人（Supervisor）作為該國的個資保護監督機關，任期 6 年即至 2014 年止。但匈牙利於 2011 年修法成立「國家個資保護與資訊自由管理局（National Authority for Data Protection and Freedom of Information）」為新的個資保護監督機關，並於該局在 2012 年成立時一併指派新的機關首長，任期 9 年。歐盟執委會認為匈牙利政府此舉**牴觸《個人資料保護指令》第 28 條第 1 項對於各會員國個資保護監督機關須有「完全之獨立性」的要求**，因此請求歐洲法院宣告匈牙利政府違背

[73] European Court of Justice, Case C-614/10, *Commission v. Austria*, 2012, para61, "…The fact that the office is composed of officials of the Federal Chancellery, which is itself subject to supervision by the DSK, carries a risk of influence over the decisions of the DSK".

[74] European Court of Justice, Case C-614/10, *Commission v. Austria*, 2012, para63, "Such a right to information is also liable to subject the DSK to indirect influence from the Federal Chancellor".

[75] European Court of Justice, Case C-614/10, *Commission v. Austria*, 2012, para63, "…the right to information set out in Article 20(2) of the BVG and Paragraph 38(2) of the DSG 2000 precludes the DSK from being capable of being regarded as operating, in all circumstances, above all suspicion of partiality".

法律義務。

歐盟執委會主張，雖然會員國得自由立法規定個資保護監督機關首長的任期，但一旦立法規定後，會員國即應受其拘束，除非有得撤換且可客觀檢驗之理由，否則便不可於任期屆滿前更換首長[76]；且匈牙利政府亦無法證實原個資保護監察人無意續任新成立的個資保護監督機關首長至原任期屆滿[77]。因此認定匈牙利政府之行為侵害個資保護監督機關之人事獨立性。

匈牙利政府則抗辯，成立新的個資保護監督機關取代原個資保護監察人，係透過憲法程序訂立於基本法（Fundamental Law）中，並質疑《個人資料保護指令》第 28 條第 1 項要求的個資保護監督機關獨立性應不包含拘束會員國成立監督機關的組織形式及其變更[78]，會員國應有權自行決定政府組織架構。

對此，**歐洲法院**於審理後提出下列說明並作出判斷：

---

[76] European Court of Justice, Case C-288/12, *Commission v. Hungary*, 2014, para38, "However, once that term has been set, the Member State must respect it and cannot compel the office to be vacated before the expiry of that term, except for overriding and objectively verifiable reasons".

[77] European Court of Justice, Case C-288/12, *Commission v. Hungary*, 2014, para39, "Hungary has not established that the Supervisor had waived the right to serve his full term of office and refused to manage the Authority".

[78] European Court of Justice, Case C-288/12, *Commission v. Hungary*, 2014, para41, "Hungary has doubts as to whether the requirement of independence set out in Article 28 of Directive 95/46 extends to the decision of a Member State on the form, or a change in the form, that the supervisory authority is to take".

A. 歐洲法院重申，功能上的獨立性尚不足使個資保護監督機關避免所有外部影響。

B. 即便只有極小風險（mere risk）會發生政府監管機關以政治力影響個資保護監督機關作出之決定，也已足夠削減個資保護監督機關執行職務的獨立性，因為將造成個資保護監督機關在作出決定時存有「**事前遵循（prior compliance）**」執行監管機關意旨的可能，也因此無法避免該監督機關沒有偏頗之虞。

C. 如果允許會員國強制個資保護監督機關提前終止任期，即可能導致個資保護監督機關以某種形式事前遵循外在政治力之意旨，將侵害獨立性之要求[79]。

D. 誠然，會員國有權自由決定行政機關的組織模式，但同時須確保遵循《個人資料保護指令》對於個資保護監督機關要求的獨立性，在本案中，即是須讓原個資保護監察人續任至其任期屆滿為止[80]。

---

[79] European Court of Justice, Case C-288/12, *Commission v. Hungary*, 2014, para54, "…If it were permissible for every Member State to compel a supervisory authority to vacate office before serving its full term, in contravention of the rules and safeguards established in that regard by the legislation applicable, the threat of such premature termination to which that authority would be exposed throughout its term of office could lead it to enter into a form of prior compliance with the political authority, which is incompatible with the requirement of independence".

[80] European Court of Justice, Case C-288/12, *Commission v. Hungary*, 2014, para60, "It is true that Member States are free to adopt or amend the institutional model that they consider to be the most appropriate for their supervisory authorities. In doing so, however, they must ensure that the independence of the supervisory authority under the second subparagraph of Article 28(1) of Directive 95/46 is not compromised, which entails the obligation to allow that authority to serve its

基於上述理由，**歐洲法院認為匈牙利政府之行為侵害《個人資料保護指令》對會員國個資保護監督機關要求的「完全之獨立性」**。

四、監督機關成員一般性條件

依《個資保護規則》規定，會員國應經由透明程序，由國會、政府、國家元首或經會員國法律委託任命的獨立機關任命其監督機關之成員[81]。而各成員應具備執行職務及行使職權所需之資格、經驗與能力（特別是個資保護領域）[82]。

監督機關成員應依會員國法律規定，於其任期屆滿、辭職或強制退休時終止其任務[83]，且僅在發生嚴重不當行為或不再具備執行其任務所需條件時始能被解雇[84]。

五、監督機關組織規範

依《個資保護規則》規定，各會員國應於內國法律中規定下列事項[85]：

---

full term of office".

81 EU, GDPR, Article53.1, "Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by: — their parliament; — their government; — their head of State; or — an independent body entrusted with the appointment under Member State law".

82 EU, GDPR, Article53.2, "Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers".

83 EU, GDPR, Article53.3, "The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned".

84 EU, GDPR, Article53.4, "A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties".

85 EU, GDPR, Article54.1, "Each Member State shall provide by law for all of the following: (a) the establishment of each supervisory authority; (b) the qualifications and eligibility conditions required to be appointed as member of each supervisory authority; (c) the rules and procedures for the appointment of the member or members of each supervisory authority; (d) the duration of the term of the member or members of each supervisory authority of no less than four years, except for the

1、各監督機關的設立。

2、擔任各監督機關成員的資格及候選條件。

3、任命各監督機關成員的規定及程序。

4、監督機關成員不少於 4 年之任期，但為維持監督機關之獨立性所必要者，自 2016 年 5 月 24 日始初任之監督機關成員任期可少於前述 4 年規定。

5、各監督機關成員得否連任及連任次數。

6、各監督機關成員及職員的義務、禁止在任內與任後為特定行為、擔任特定職位、收受不當利益，以及終止雇用之規則等條件。

又各監督機關之成員及人員應依歐盟法律或內國法律規定，在其任內及離職後，對因履行任務或行使職權所知悉之任何機密資訊負有保密義務。前述保密義務特別適用於其在任時受理提報違反《個資保護規則》情事之自然人資訊[86]。

---

first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure; (e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment; (f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment".

[86] EU, GDPR, Article54.2, "The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation".

六、監督機關之管轄、任務與職權

(一) 監督機關及最高監督機關之管轄

依《個資保護規則》規定，各監督機關在其所屬會員國境內均有權執行規則授予之任務及行使其職權[87]。但對法院行使司法權所為之處理個資行為無管轄權[88]。

資料控制者或受託者的（主）營業處所之監督機關應就資料控制者或受託者跨境處理個資之行為擔任最高監督機關，並遵循依《個資保護規則》第 60 條（最高監督機關與其他該管監督機關之合作）相關規定[89]，且該最高監督機關係資料控制者或受託者跨境處理個資行為之專責機關[90]。

但如某跨境處理個資事件僅與資料控制者或受託者在某會員國的營業處所有關，或僅明顯影響某會員國的資料當事人時，該會員國之監督機關就此跨境處理個資行為亦有權受理申訴或舉報對《個資保護規則》的潛在侵害[91]。

在前述情況下，該監督機關應將此事件即時通報最高監

---

87 EU, GDPR, Article55.1, "Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State".

88 EU, GDPR, Article55.3, "Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity".

89 EU, GDPR, Article56.1, "Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60".

90 EU, GDPR, Article56.6, "The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor".

91 EU, GDPR, Article56.2, "By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State".

督機關。最高監督機關在受通知後 3 週內，應考量資料控制者或受託者是否在通報該事件的監督機關所在會員國內設有營業處所，以決定是否依《個資保護規則》第 60 條（最高監督機關與其他該管監督機關之合作）相關規定處理該事件[92]。

如最高監督機關決定處理該事件，即應適用《個資保護規則》第 60 條規定之程序。通報該事件的監督機關得向最高監督機關提交對該事件所為決定之草稿，最高監督機關在依《個資保護規則》第 60 條第 3 項準備最終決定的草稿時，應在最大程度內參酌監督機關於該草稿內提出之意見[93]。但若最高監督機關決定不處理該事件，通報該事件的監督機關應依《個資保護規則》第 61 條（監督機關的互助）及第 62 條（監督機關的聯合行動）自行處理該事件[94]。

(二) 監督機關之任務

除《個資保護規則》另有規定外，各監督機關在其管轄領域內應執行下列任務[95]：

---

[92] EU, GDPR, Article56.3, "In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it".

[93] EU, GDPR, Article56.4, "Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3)".

[94] EU, GDPR, Article56.5, "Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62".

[95] EU, GDPR, Article57.1, "Without prejudice to other tasks set out under this Regulation, each

1、監督並實施《個資保護規則》之適用。

2、提升公民對於處理個資的風險、規則、安全維護、當事人權利的意識。並應特別留意專對孩童之行為。

3、依照會員國法律對國會、政府和其他機構、法人提出關於處理個資時相關的自然人權利與自由保護的立法及行政措施。

4、提升資料控制者與受託者對《個資保護規則》所定義務

---

supervisory authority shall on its territory:(a)monitor and enforce the application of this Regulation; (b)promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention; (c)advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing; (d)promote the awareness of controllers and processors of their obligations under this Regulation; (e)upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end; (f)handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary; (g)cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation; (h)conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority; (i)monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices; (j)monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices; (k)establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4); (l)give advice on the processing operations referred to in Article 36(2); (m)encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5); (n)encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5); (o)where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7); (p)draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43; (q)conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43; (r)authorise contractual clauses and provisions referred to in Article 46(3); (s)approve binding corporate rules pursuant to Article 47; (t)contribute to the activities of the Board; (u)keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and (v)fulfil any other tasks related to the protection of personal data".

之認知。

5、依資料當事人要求對其提供《個資保護規則》所定有關當事人行使權利之資訊，並於適當時與他國監督機關合作以達此目的。

6、處理資料當事人或法人、組織、協會依《個資保護規則》第 80 條提出之申訴，並在適當範圍內對申訴事件進行調查，且在合理期間內對申訴人通知調查程序及結果，特別是針對需要進一步調查或與其他監督機關協調的情況。各監督機關應盡力促成本申訴程序之實現，例如制定以電子形式或其他通訊方式完成的申訴表格[96]。

7、與其他監督機關合作，包含資訊共享及互相協助，以確保《個資保護規則》適用及執行的一致性。

8、對《個資保護規則》之適用執行調查，包含對來自其他監督機關或公務機關之資訊。

9、掌握對個資保護具有影響的相關發展，特別是資通訊技術及商業實務的發展。

10、通過《個資保護規則》第 28 條第 8 項及第 46 條第 2 項第 d 款的標準契約條款。

11、制定並維護依《個資保護規則》第 35 條第 4 項所定應執行個資保護衝擊評估之處理個資行為的列表。

[96] EU, GDPR, Article57.2, "Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication".

12、依《個資保護規則》第 36 條第 2 項規定，答覆資料控制者執行「個資保護衝擊評估」後提出之諮詢。

13、鼓勵依《個資保護規則》第 40 條第 1 項制定實務指引，並依《個資保護規則》第 40 條第 5 項對該提供足夠安全防護的實務指引提供意見及許可。

14、鼓勵依《個資保護規則》第 42 條第 1 項建置資料保護認證機制及資料保護標章，並依《個資保護規則》第 42 條第 5 項對許可該認證之標準。

15、如有適用，定期檢查依《個資保護規則》第 42 條第 7 項發布之認證。

16、起草並出版對依本規則第 41 條負責監督實務指引之法人的委任標準及依本規則第 43 條負責認證之法人的委任標準。

17、執行對依《個資保護規則》第 41 條負責監督實務指引之法人及依《個資保護規則》第 43 條負責認證之法人的委任。

18、授權《個資保護規則》第 46 條第 3 項之契約條款及規定。

19、許可《個資保護規則》第 47 條的約束性企業規則（binding corporate rules）。

20、協助歐盟個資保護委員會之活動。

21、將違反《個資保護規則》之事件及依本規則第 58 條第

2 項採取的對應措施作成內部紀錄。

22、執行其他任何與個資保護有關之任務。

(三) 監督機關之職權

依《個資保護規則》規定，監督機關應依適當措施行使下述職權，包含依歐盟及會員國法律規定之有效的司法補償及正當程序[97]。

各會員國應以法律授與監督機關得將違反《個資保護規則》之事件提報司法機關之權及發起或參與其他法律程序以落實《個資保護規則》之權（如適當）[98]。

各會員國得以法律授與監督機關行使下列「調查權」、「糾正權」及「批准及建議權」以外之其他職權，但不得減損《個資保護規則》第 7 章規範（監督機關之合作與一致）的有效性[99]。

各監督機關之職權如下：

1、各監督機關有下列調查權[100]：

---

[97] EU, GDPR, Article58.4, "The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter".

[98] EU, GDPR, Article58.5, "Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation".

[99] EU, GDPR, Article58.6, "Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII".

[100] EU, GDPR, Article58.1, "Each supervisory authority shall have all of the following investigative powers: (a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks; (b) to carry out investigations in the form of data protection audits; (c) to carry out a review on

(1) 為執行職權而要求資料控制者或受託者，或資料控制者或受託者之代表人提供任何資訊。

(2) 以個資保護稽核形式發起調查。

(3) 審查依《個資保護規則》第 42 條第 7 項發布之認證

(4) 將違反《個資保護規則》之侵害事件通知資料控制者或受託者

(5) 為執行任務而由資料控制者或受託者獲得存取所有個人資料及所有資訊的權限

(6) 在符合歐盟或會員國程序法的前提下，訪查資料控制者或受託者的任何處所，包括任何處理個資的設備或工具。

2、 各監督機關有下列糾正權[101]：

---

certifications issued pursuant to Article 42(7); (d) to notify the controller or the processor of an alleged infringement of this Regulation; (e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks; (f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law".

[101] EU, GDPR, Article58.2, "Each supervisory authority shall have all of the following corrective powers: (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation; (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation; (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation; (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period; (e) to order the controller to communicate a personal data breach to the data subject; (f) to impose a temporary or definitive limitation including a ban on processing; (g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19; (h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met; (i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case; (j) to order the suspension of data flows to a recipient in a third country or to an international

(1) 對將做出可能違反《個資保護規則》的處理個資行為之資料控制者或受託者發布警示。

(2) 對已做出違反《個資保護規則》的處理個資行為之資料控制者或受託者為告誡（reprimand）處分。

(3) 命令資料控制者或受託者滿足資料當事人依《個資保護規則》實行權利之請求。

(4) 命令資料控制者或受託者使其處理個資之行為符合《個資保護規則》,如可適當指定特定方式及期間。

(5) 命令資料控制者向資料當事人通知個資侵害事故。

(6) 作出暫時或最終之限制，包含禁止處理個資。

(7) 命令依《個資保護規則》第 16 條、第 17 條、第 18 條更正、刪除個資或限制處理個資，及依第 17 條第 2 項與第 19 條對曾揭露個資之對象通知前述情況。

(8) 依《個資保護規則》第 42 條及第 43 條撤銷或命認證機關撤銷認證，或命認證機關不得發證予無法符合或不再符合條件之申請者。

(9) 依具體個案情況，除採取本項各款行為外，亦可逕行或同時依《個資保護規則》第 83 條處以罰鍰。

(10) 命令禁止將個人資料傳輸至第三國或跨國組織。

---

organisation".

3、各監督機關有下列各項批准及建議權[102]：

(1) 對資料控制者依《個資保護規則》第 36 條提出的前期諮詢提出建議。

(2) 主動或依請求對任何與個資保護有關之事項向國家議會（national parliament）、會員國政府或依會員國法律向其他機構或機關以及公眾發布意見。

(3) 依會員國法律規定，依《個資保護規則》第 36 條第 5 項批准處理個資。

(4) 依《個資保護規則》第 40 條第 5 項發布意見並認可實務指引的草稿。

(5) 依《個資保護規則》第 43 條指派認證機關。

(6) 依《個資保護規則》第 42 條第 5 項授予認證及認可授證之條件。

(7) 依《個資保護規則》第 28 條第 8 項及第 46 條第 2 項第 d 款通過標準個資保護條款。

---

[102] EU, GDPR, Article58.3, "Each supervisory authority shall have all of the following authorisation and advisory powers: (a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36; (b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data; (c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation; (d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5); (e) to accredit certification bodies pursuant to Article 43; (f) to issue certifications and approve criteria of certification in accordance with Article 42(5); (g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2); (h) to authorise contractual clauses referred to in point (a) of Article 46(3); (i) to authorise administrative arrangements referred to in point (b) of Article 46(3); (j) to approve binding corporate rules pursuant to Article 47".

(8) 依《個資保護規則》第 46 條第 3 項第 a 款批准契約條款。

(9) 依《個資保護規則》第 46 條第 3 項第 b 款批准行政協議（administrative arrangements）。

(10) 依《個資保護規則》第 47 條認可約束性契約規則（binding corporate rules）。

七、監督機關業務活動報告

各監督機關應將其業務活動提出年度報告，內容得包含各類事故通知清單及依《個資保護規則》第 58 條第 2 項採取之各類措施，並應依會員國法律指定，將報告提交國家議會、政府及其他監督機關，且應將報告公開及提供歐盟執委會及個資保護委員會[103]。

[103] EU, GDPR, Article59, "Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board".

第二節　英國—資訊委員辦公室（ICO）

一、概述

英國於個人資料保護法（Data Protection Act 1998）第 6 條創設「資訊委員（Information Commissioner）」一職[104]，由英國女王任命[105]，並以該法的附表（Schedule）5 明定資訊委員的組織規範[106]。

英國資訊委員辦公室（Information Commissioner's Office，以下簡稱 ICO）係一「非部會公務機關（non-departmental public body）之行政法人（半官方機構）」，由英國文化、媒體及體育部（Department for Culture, Media and Sport）資助成立[107]，除在英國柴郡（Cheshire）威姆斯洛（Wilmslow）的總部之外，亦分別設有蘇格蘭（Scotland）辦公室、威爾斯（Wales）辦公室及北愛爾蘭（Northern Ireland）辦公室。

ICO 原成立於 1984 年，作為英國個資保護登記機關，在英國於 1998 年施行個人資料保護法後，即繼受成為英國的個資保護專責機關，監管個人資料保護法的施行。

二、監管對象與主管法規

英國個人資料保護法規範之主體包含公務機關及非公務機

---

[104] UK, Data Protection Act, Section 6(1), "For the purposes of this Act and of the Freedom of Information Act 2000 there shall be an officer known as the Information Commissioner (in this Act referred to as “the Commissioner”)".

[105] UK, Data Protection Act, Section 6(2), "The Commissioner shall be appointed by Her Majesty by Letters Patent".

[106] UK, Data Protection Act, Section 6(7), "Schedule 5 has effect in relation to the Commissioner".

[107] 見 https://ico.org.uk/about-the-ico/who-we-are/relationship-with-the-dcms/，最後到訪日為 106 年 7 月 3 日。

關，因此，公務機關亦是英國資訊委員的監管對象，並得依法處以罰款。

除個人資料保護法外，英國資訊委員亦職司《資訊自由法（Freedom of Information Act）》、《隱私與電子通訊規則（Privacy and Eletronic Communications Regulations）》、《環境資訊規則（Environmental Information Regulations）》、《歐洲共同體空間資訊規則（INSPIRE Regulations）》、《內部市場電子交易驗證與信任服務規則（Eidas Regulation）》、《公部門資訊再利用規則（Re-use of Public Sector Regulations）》及《歐盟個人資料保護指令（GDPR）》的監管實施。

三、組織規範

(一) 地位

依英國個人資料保護法附表 5 規定，資訊委員及其官員（Officer）與職員（Staff）均非皇家政府（Crown）的公務員或代理人[108]。

(二) 任免

資訊委員之人選應經由公平公開之合法程序競爭擇定後推薦予英國女王任命[109]，其任期自受任起不超過 7 年[110]，

[108] UK, Data Protection Act, Schedule5, Paragraph1(2), "The Commissioner and his officers and staff are not to be regarded as servants or agents of the Crown".

[109] UK, Data Protection Act, Schedule5, Paragraph2(3B), "No recommendation may be made to Her Majesty for the appointment of a person as the Commissioner unless the person concerned has been selected on merit on the basis of fair and open competition".

[110] UK, Data Protection Act, Schedule5, Paragraph2(1), "Subject to the provisions of this paragraph, the Commissioner shall hold office for such term not exceeding seven years as may be determined at the time of his appointment".

不得連任或再任[111]。

資訊委員可主動請求英國女王解除其職務[112]，或被動由英國女王依兩議院提出之要求而免職[113]，惟除有皇家國務大臣認定資訊委員有下列情況之一而向任一議院提出報告之外，任一議院均不得提出免職資訊委員之動議[114]：

1、該資訊委員連續3個月以上未能使資訊委員辦公室執行其功能[115]。

2、該資訊委員無法符合任命之條件[116]。

3、該資訊委員獲刑事有罪判決[117]。

4、該資訊委員處於破產狀態且尚未被免除債務，或其財產於蘇格蘭地區遭扣押且尚未被免除債務[118]。

5、該資訊委員與債權人達成協議或與其簽署和解契約或信託契約[119]。

---

[111] UK, Data Protection Act, Schedule5, Paragraph2(3C), "A person appointed as the Commissioner may not be appointed again for a further term of office".

[112] UK, Data Protection Act, Schedule5, Paragraph2(2), "The Commissioner may be relieved of his office by Her Majesty at his own request".

[113] UK, Data Protection Act, Schedule5, Paragraph2(3), "The Commissioner may be removed from office by Her Majesty in pursuance of an Address from both Houses of Parliament".

[114] UK, Data Protection Act, Schedule5, Paragraph2(3A), "No motion is to be made in either House of Parliament for such an Address unless a Minister of the Crown has presented a report to that House stating that the Minister is satisfied that one or more of the following grounds is made out".

[115] UK, Data Protection Act, Schedule5, Paragraph2(3A)(a), "the Commissioner has failed to discharge the functions of the office for a continuous period of at least 3 months".

[116] UK, Data Protection Act, Schedule5, Paragraph2(3A)(b), "the Commissioner has failed to comply with the terms of appointment".

[117] UK, Data Protection Act, Schedule5, Paragraph2(3A)(c), "the Commissioner has been convicted of a criminal offence".

[118] UK, Data Protection Act, Schedule5, Paragraph2(3A)(d), "the Commissioner is an undischarged bankrupt or the Commissioner's estate has been sequestrated in Scotland and the Commissioner has not been discharged".

[119] UK, Data Protection Act, Schedule5, Paragraph2(3A)(e), "the Commissioner has made an

6、其他可認該資訊委員已不適任或無法發揮資訊委員辦公室之功能的情況[120]。

(三) 薪俸

資訊委員（得由下議院決議）應為有給職，且應得請領退休金[121]，均由統一公債基金支付（Consolidated Fund）[122]。前述下議院決議得：

1、具體規範薪資及退休金內容[123]。

2、規定該薪資或退休金與皇家政府特定機關或特定職位之人員相同或以相同基準計算[124]。

3、具體規範該薪資或退休金並於決議中規定得依何種因素增加金額[125]。

又該決議得於通過之日起生效，或依其規定於通過之日前或後之特定日期生效[126]。另該決議得就退休金部分訂定個

---

arrangement or composition contract with, or has granted a trust deed for, the Commissioner's creditors".

[120] UK, Data Protection Act, Schedule5, Paragraph2(3A)(f), "the Commissioner is otherwise unfit to hold the office or unable to carry out its functions".

[121] UK, Data Protection Act, Schedule5, Paragraph3(1), "There shall be paid—(a)to the Commissioner such salary, and(b)to or in respect of theCommissioner such pension,as may be specified by a resolution of the House of Commons".

[122] UK, Data Protection Act, Schedule5, Paragraph3(5), "Any salary or pension payable under this paragraph shall be charged on and issued out of the Consolidated Fund".

[123] UK, Data Protection Act, Schedule5, Paragraph3(2)(a), "specify the salary or pension".

[124] UK, Data Protection Act, Schedule5, Paragraph3(2)(b), "provide that the salary or pension is to be the same as, or calculated on the same basis as, that payable to, or to or in respect of, a person employed in a specified office under, or in a specified capacity in the service of, the Crown, or".

[125] UK, Data Protection Act, Schedule5, Paragraph3(2)(c), "specify the salary or pension and provide for it to be increased by reference to such variables as may be specified in the resolution".

[126] UK, Data Protection Act, Schedule5, Paragraph3(3), "A resolution for the purposes of this paragraph may take effect from the date on which it is passed or from any earlier or later date specified in the resolution".

別資訊委員適用之規範[127]。

(四) 成員

資訊委員應指派一至二位副資訊委員[128]，且在指派第二位副資訊委員時，應具體說明兩位副資訊委員應負責執行之資訊委員功能為何[129]。資訊委員並得自行決定其他成員的人數[130]，以及副資訊委員與其他成員之薪資及其他條件[131]。

副資訊委員應在資訊委員缺位或因任何原因無法行使職權時，執行個人資料保護法及資訊公開法（Freedom of Information Act 2000）賦予資訊委員之任務[132]。又在不影響前述規範的前提下，資訊委員得將其依《個人資料保護法》及《資訊公開法》賦予之任務授權資訊委員辦公室任何一位成員執行[133]。

資訊委員在指派職位時，應考量合法程序的公平公開

---

[127] UK, Data Protection Act, Schedule5, Paragraph3(4), "A resolution for the purposes of this paragraph may make different provision in relation to the pension payable to or in respect of different holders of the office of Commissioner".

[128] UK, Data Protection Act, Schedule5, Paragraph4(1)(a), "shall appoint a deputy commissioner or two deputy commissioners".

[129] UK, Data Protection Act, Schedule5, Paragraph4(1A), "The Commissioner shall, when appointing any second deputy commissioner, specify which of the Commissioner's functions are to be performed, in the circumstances referred to in paragraph 5(1), by each of the deputy commissioners".

[130] UK, Data Protection Act, Schedule5, Paragraph4(1)(b), "may appoint such number of other officers and staff as he may determine".

[131] UK, Data Protection Act, Schedule5, Paragraph4(2), "The remuneration and other conditions of service of the persons appointed under this paragraph shall be determined by the Commissioner".

[132] UK, Data Protection Act, Schedule5, Paragraph5(1), "The deputy commissioner or deputy commissioners shall perform the functions conferred by this Act or the Freedom of Information Act 2000 on the Commissioner during any vacancy in that office or at any time when the Commissioner is for any reason unable to act".

[133] UK, Data Protection Act, Schedule5, Paragraph5(2), "Without prejudice to sub-paragraph (1), any functions of the Commissioner under this Act or the Freedom of Information Act 2000 may, to the extent authorised by him, be performed by any of his officers or staff".

原則競爭後以擇定人選[134]。

(五) 款項

資訊委員因執行職務所取得之任何款項均應交付內閣大臣，但內閣大臣經財政部同意另有指示者不在此限。內閣大臣應將資訊委員交付之款項轉付統一公債基金[135]。

(六) 帳目

資訊委員應保存適當帳目及相關紀錄[136]，並應依內閣大臣指定之形式備妥各財務年度（每年 4 月 1 日起算 12 個月[137])的說明[138]，同時將該說明副本於次年度 8 月 31 日(前）或依財政部指示於該年度終了日（前）提交審計官及審計長（Comptroller and Auditor General）[139]。審計官及審計長應檢視並核實資訊委員提出之說明並將該說明作為提交予兩議院之附件[140]。

---

[134] UK, Data Protection Act, Schedule5, Paragraph4(4A), "In making appointments under this paragraph, the Commissioner must have regard to the principle of selection on merit on the basis of fair and open competition".

[135] UK, Data Protection Act, Schedule5, Paragraph9,"(1)All fees and other sums received by the Commissioner in the exercise of his functions under this Act under section 159 of the Consumer Credit Act 1974 or under the Freedom of Information Act 2000shall be paid by him to the Secretary of State.(2)Sub-paragraph (1) shall not apply where the Secretary of State , with the consent of the Treasury, otherwise directs.(3)Any sums received by the Secretary of Stateunder sub-paragraph (1) shall be paid into the Consolidated Fund".

[136] UK, Data Protection Act, Schedule5, Paragraph10(1)(a), "to keep proper accounts and other records in relation to the accounts".

[137] UK, Data Protection Act, Schedule5, Paragraph10(3), "In this paragraph “financial year” means a period of twelve months beginning with 1st April".

[138] UK, Data Protection Act, Schedule5, Paragraph10(1)(b), "to prepare in respect of each financial year a statement of account in such form as the Secretary of State may direct".

[139] UK, Data Protection Act, Schedule5, Paragraph10(1)(c), "to send copies of that statement to the Comptroller and Auditor General on or before 31st August next following the end of the year to which the statement relates or on or before such earlier date after the end of that year as the Treasury may direct".

[140] UK, Data Protection Act, Schedule5, Paragraph10(2), "The Comptroller and Auditor General shall examine and certify any statement sent to him under this paragraph and lay copies of it together

(七) 組織架構

現行 ICO 的組織架構除資訊委員及兩位副資訊委員外，設有下列各內部單位：

1、客戶與商業服務（Customer and Business Services）

2、財務（Finance）

3、優良實務（Good Practice）

4、執法（Enforcement）

5、分部管理（ICO Regions）

6、組織發展（Organisational Development）

7、合作事務（Corporate Affairs）

8、策略聯繫（Strategic Liaison）

9、成果精進（Performance Improvement）

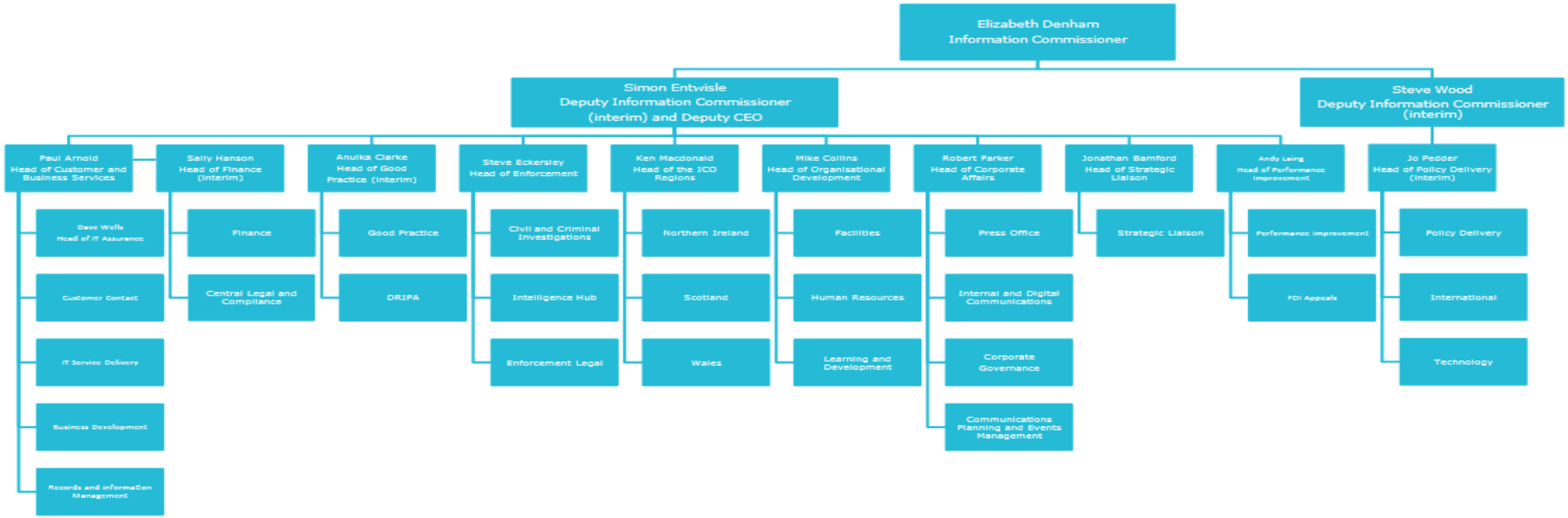
10、 政策宣導（Policy Delivery）

---

with his report thereon before each House of Parliament".

圖 1 英國資訊委員辦公室組織架構圖

Organisational structure



ico.
Information Commissioner's Office

19/07/2016

四、法定職務

(一) 執行通知（Enforcement notices）

如資訊委員認為資料控制者已經或正在違反個人資料保護法規定之各項原則時，應考量該違反行為是否已對或將對任何人造成損害[141]，以決定是否對該資料控制者發出「執行通知」，要求其於期限內採取特定之行為，或於期限屆滿後禁止進行特定之行為，甚至是在期限屆滿後禁止蒐集、處理、利用任何或特定個人資料，或基於某目的或以某方式蒐集、處理、利用個人資料[142]。

執行通知內容應包含「資訊委員認為資料控制者已違反或正在違反的個資保護原則及其理由」與「資料控制者得向法院聲明不服之權利」[143]。

此外，如資訊委員係因資料控制者未更正或刪除不正確的個資而作出執行通知時，該執行通知內容得包含要求該資料控制者更正或刪除該不正確個資，並應敘明理由[144]。

---

[141] UK, Data Protection Act, Section40(2), "In deciding whether to serve an enforcement notice, the Commissioner shall consider whether the contravention has caused or is likely to cause any person damage or distress".

[142] UK, Data Protection Act, Section40(1), "If the Commissioner is satisfied that a data controller has contravened or is contravening any of the data protection principles, the Commissioner may serve him with a notice (in this Act referred to as “an enforcement notice”) requiring him, for complying with the principle or principles in question, to do either or both of the following—(a)to take within such time as may be specified in the notice, or to refrain from taking after such time as may be so specified, such steps as are so specified, or(b)to refrain from processing any personal data, or any personal data of a description specified in the notice, or to refrain from processing them for a purpose so specified or in a manner so specified, after such time as may be so specified".

[143] UK, Data Protection Act, Section40(6), "An enforcement notice must contain—(a)a statement of the data protection principle or principles which the Commissioner is satisfied have been or are being contravened and his reasons for reaching that conclusion, and(b)particulars of the rights of appeal conferred by section 48".

[144] UK, Data Protection Act, Section40(3), "An enforcement notice in respect of a contravention of the fourth data protection principle which requires the data controller to rectify, block, erase or destroy

又執行通知不得要求資料控制者在聲明不服期間屆滿前即遵照辦理，如資料控制者依法聲明不服時，在判決作出或撤回聲明前，均無須遵從執行通知內容[145]。但如資訊委員有理由因特殊情況認為要求資料控制者遵守執行通知具急迫性時，得在執行通知中敘明該情形並附理由後要求資料控制者即時（但不得少於執行通知送達日起算 7 日）遵照辦理，不受前述規定限制[146]。

如資訊委員認為執行通知中的全部或任一要求已無遵守之必要時，得以書面取消或變更執行通知內容。任何收受執行通知之人亦得在聲明不服期間經過後，基於情況變更而執行通知中的全部或任一要求已無遵守必要之理由，隨時以書面向資訊委員請求取消或變更執行通知內容[147]。

(二) 評估通知（Assessmentnotices）

---

any inaccurate data may also require the data controller to rectify, block, erase or destroy any other data held by him and containing an expression of opinion which appears to the Commissioner to be based on the inaccurate data".

145 UK, Data Protection Act, Section40(7), "Subject to subsection (8), an enforcement notice must not require any of the provisionsof the notice to be complied with before the end of the period within which an appealcan be brought against the notice and, if such an appeal is brought, the notice need notbe complied with pending the determination or withdrawal of the appeal".

146 UK, Data Protection Act, Section40(8), "If by reason of special circumstances the Commissioner considers that an enforcementnotice should be complied with as a matter of urgency he may include in the noticea statement to that effect and a statement of his reasons for reaching that conclusion;and in that event subsection (7) shall not apply but the notice must not require theprovisions of the notice to be complied with before the end of the period of seven daysbeginning with the day on which the notice is served".

147 UK, Data Protection Act, Section41, " (1)If the Commissioner considers that all or any of the provisions of an enforcement notice need not be complied with in order to ensure compliance with the data protection principle or principles to which it relates, he may cancel or vary the notice by written notice to the person on whom it was served.(2)A person on whom an enforcement notice has been served may, at any time after the expiry of the period during which an appeal can be brought against that notice, apply in writing to the Commissioner for the cancellation or variation of that notice on the ground that, by reason of a change of circumstances, all or any of the provisions of that notice need not be complied with in order to ensure compliance with the data protection principle or principles to which that notice relates".

資訊委員得對下列對象作出「評估通知」[148]，以讓資訊委員評估該資料控制者是否遵守個資保護原則[149]：

1、政府部門。

2、依內閣大臣命令適用之公務機關，但內閣大臣應不超過每5年之期間重新檢視該公務機關是否仍適合接受評估[150]。

3、依內閣大臣命令適用之特定種類之人，但內閣大臣須經資訊委員提出建議且內閣大臣徵詢該種類之人的代表人或其他適當之人之意見後，始得命令適用[151]；且內閣大臣或資訊委員應考量「該種類之人控制之個資性質與數量」及「該種類之人違反個資保護原則可能造成的損害」等因素以決定是否有必要指定或建議該種類之人作為接受評估通知之對象[152]。又內閣大臣應不超過每5年

---

[148] UK, Data Protection Act, Section41A(2), " A data controller is within this subsection if the data controller is—(a)a government department,(b)a public authority designated for the purposes of this section by an order made by the Secretary of State, or(c)a person of a description designated for the purposes of this section by such an order".

[149] UK, Data Protection Act, Section41A(1), "The Commissioner may serve a data controller within subsection (2) with a notice (in this Act referred to as an "assessment notice") for the purpose of enabling the Commissioner to determine whether the data controller has complied or is complying with the data protection principles".

[150] UK, Data Protection Act, Section41A(8), "Where a public authority has been designated by an order under subsection (2)(b) the Secretary of State must reconsider, at intervals of no greater than 5 years, whether it continues to be appropriate for the authority to be designated".

[151] UK, Data Protection Act, Section41A(9), "The Secretary of State may not make an order under subsection (2)(c) which designates a description of persons unless—(a)the Commissioner has made a recommendation that the description be designated, and(b)the Secretary of State has consulted—(i)such persons as appear to the Secretary of State to represent the interests of those that meet the description;(ii)such other persons as the Secretary of State considers appropriate".

[152] UK, Data Protection Act, Section41A(10), "The Secretary of State may not make an order under subsection (2)(c), and the Commissioner may not make a recommendation under subsection (9)(a), unless the Secretary of State or (as the case may be) the Commissioner is satisfied that it is necessary for the description of persons in question to be designated having regard to—(a)the nature and quantity of data under the control of such persons, and(b)any damage or distress which may be caused by a contravention by such persons of the data protection principles".

之期間依前述因素重新檢視該種類之人是否仍適合接受評估[153]。

前述評估通知應包含下列全部或任一要求事項[154]：

1、允許資訊委員(包含資訊委員辦公室之成員，以下同[155])進入任何指名建築物內。

2、提供資訊委員任何該建築物內的特定文件。

3、協助資訊委員審閱任何得以該建築物內之設備讀取之資訊。

4、依資訊委員要求交付「資訊委員指示提供之任何文件的複製本」或「資訊委員審閱之任何資訊（依資訊委員要求之形式）的複製本」。

5、提供資訊委員該建築物內任何指名的設備或其他工具。

---

[153] UK, Data Protection Act, Section41A(11), "Where a description of persons has been designated by an order under subsection (2)(c) the Secretary of State must reconsider, at intervals of no greater than 5 years, whether it continues to be necessary for the description to be designated having regard to the matters mentioned in subsection (10)".

[154] UK, Data Protection Act, Section41A(3), "An assessment notice is a notice which requires the data controller to do all or any of the following—(a)permit the Commissioner to enter any specified premises;(b)direct the Commissioner to any documents on the premises that are of a specified description;(c)assist the Commissioner to view any information of a specified description that is capable of being viewed using equipment on the premises;(d)comply with any request from the Commissioner for—(i)a copy of any of the documents to which the Commissioner is directed;(ii)a copy (in such form as may be requested) of any of the information which the Commissioner is assisted to view;(e)direct the Commissioner to any equipment or other material on the premises which is of a specified description;(f)permit the Commissioner to inspect or examine any of the documents, information, equipment or material to which the Commissioner is directed or which the Commissioner is assisted to view;(g)permit the Commissioner to observe the processing of any personal data that takes place on the premises;(h)make available for interview by the Commissioner a specified number of persons of a specified description who process personal data on behalf of the data controller (or such number as are willing to be interviewed)".

[155] UK, Data Protection Act, Section41A(4), "In subsection (3) references to the Commissioner include references to the Commissioner's officers and staff".

6、允許資訊委員調查或檢閱任何取得或審閱之文件、資訊、設備或工具。

7、允許資訊委員觀察在該建築物內發生的個人資料處理行為。

8、安排資訊委員指名之人員或自願之人員接受資訊委員訪談。

另評估通知內容應包含收受通知之資料控制者得依法聲明不服之權利[156]。又資訊委員得以書面通知該資料控制者取消評估通知[157]。

評估通知應就各別要求事項指明遵守之時間或期間[158]，但該時間不得落於資料控制者得聲明不服之期間，或該期間不得於資料控制仍得聲明不服之期間內起算；且如資料控制者依法聲明不服時，在判決作出或撤回聲明前，均無須遵從評估通知之要求[159]。但如資訊委員有理由因特殊情況認為要求資料控制者遵守評估通知具急迫性時，得在評估通知中敘明該情形並附理由後要求資料控制者即時（但不

[156] UK, Data Protection Act, Section41A(6), "An assessment notice must also contain particulars of the rights of appeal conferred by section 48".

[157] UK, Data Protection Act, Section41A(7), "The Commissioner may cancel an assessment notice by written notice to the data controller on whom it was served".

[158] UK, Data Protection Act, Section41A(5), "An assessment notice must, in relation to each requirement imposed by the notice, specify—(a)the time at which the requirement is to be complied with, or(b)the period during which the requirement is to be complied with".

[159] UK, Data Protection Act, Section41B(1), "A time specified in an assessment notice under section 41A(5) in relation to a requirement must not fall, and a period so specified must not begin, before the end of the period within which an appeal can be brought against the notice, and if such an appeal is brought the requirement need not be complied with pending the determination or withdrawal of the appeal".

得少於評估通知送達日起算 7 日）遵照辦理[160]。

又資訊委員應就行使「評估通知」之職權制定實務指引（code of practice）[161]，並於發布前徵詢內閣大臣之意見（修改後亦同）[162]。該指引內容應包含「如何決定是否對資料控制者發出評估通知」、「哪些文件或資訊（例如與自然人之身體、心理、社會福利等事項相關之文件或資訊[163]）不得被要求受檢或僅得由特定之人審閱檢視」、「人員受訪之事宜」、「資訊委員作出評估報告之程序」等事項[164]。

前述「評估報告」內容應包含「認定資料控制者是否已遵循或正遵循個資法規定的個資保護原則」、「為使資料控制者遵循個資保護原則所作出應作為或不作為之建議」、「其他特定事項」[165]。

---

[160] UK, Data Protection Act, Section41B(2), "If by reason of special circumstances the Commissioner considers that it is necessary for the data controller to comply with a requirement in an assessment notice as a matter of urgency, the Commissioner may include in the notice a statement to that effect and a statement of the reasons for that conclusion; and in that event subsection (1) applies in relation to the requirement as if for the words from "within" to the end there were substituted of 7 days beginning with the day on which the notice is served".

[161] UK, Data Protection Act, Section41C(1), "The Commissioner must prepare and issue a code of practice as to the manner in which the Commissioner's functions under and in connection with section 41A are to be exercised".

[162] UK, Data Protection Act, Section41C(7), "The Commissioner must consult the Secretary of State before issuing the code (or an altered or replacement code)".

[163] UK, Data Protection Act, Section41C(3), "The provisions of the code made by virtue of subsection (2)(b) must, in particular, include provisions that relate to—(a)documents and information concerning an individual's physical or mental health;(b)documents and information concerning the provision of social care for an individual".

[164] UK, Data Protection Act, Section41C(2), "The code must in particular—(a)specify factors to be considered in determining whether to serve an assessment notice on a data controller;(b)specify descriptions of documents and information that—(i)are not to be examined or inspected in pursuance of an assessment notice, or(ii)are to be so examined or inspected only by persons of a description specified in the code;(c)deal with the nature of inspections and examinations carried out in pursuance of an assessment notice;(d)deal with the nature of interviews carried out in pursuance of an assessment notice;(e)deal with the preparation, issuing and publication by the Commissioner of assessment reports in respect of data controllers that have been served with assessment notices".

[165] UK, Data Protection Act, Section41C(4), "An assessment report is a report which contains—(a)a determination as to whether a data controller has complied or is complying with the data protection

(三) 評估請求（Request for assessment）

任何人如（認為自己）正因資料控制者處理個資之行為而受有直接影響時，均得自行或委託他人向資訊委員請求評估該處理個資行為是否符合《個人資料保護法》[166]。

除非資訊委員經合理要求後仍未獲得「確認請求評估者之身分」及「辨別系爭個資處理行為」之足夠資訊，否則資訊委員於收受評估請求後即應以其認為合適之方式執行評估[167]。

資訊委員在考量前述「合適之方式」時，應斟酌下列事項[168]：

1、該請求本意所及之範圍。

2、該請求是否不當遲延。

3、該評估請求者之請求是否得由《個人資料保護法》第 7 條（當事人請求接取個資之權利）獲得滿足。

---

principles,(b)recommendations as to any steps which the data controller ought to take, or refrain from taking, to ensure compliance with any of those principles, and(c)such other matters as are specified in the code".

166 UK, Data Protection Act, Section42(1), "IA request may be made to the Commissioner by or on behalf of any person who is, or believes himself to be, directly affected by any processing of personal data for an assessment as to whether it is likely or unlikely that the processing has been or is being carried out in compliance with the provisions of this Act".

167 UK, Data Protection Act, Section42(2), "On receiving a request under this section, the Commissioner shall make an assessment in such manner as appears to him to be appropriate, unless he has not been supplied with such information as he may reasonably require in order to—(a)satisfy himself as to the identity of the person making the request, and(b)enable him to identify the processing in question".

168 UK, Data Protection Act, Section42(3), "The matters to which the Commissioner may have regard in determining in what manner it is appropriate to make an assessment include—(a)the extent to which the request appears to him to raise a matter of substance,(b)any undue delay in making the request, and(c)whether or not the person making the request is entitled to make an application under section 7 in respect of the personal data in question".

資訊委員於接受評估請求後，應告知該請求者其是否依請求作出評估，並在適當之範圍將資訊委員之意見及採取之措施告知該請求者[169]。

(四) 資訊請求通知（Information notices）

如資訊委員「接受評估請求」或「為認定資料控制者是否已遵循或正在遵循個資保護原則而須合理要求資料控制者提供資訊」時，得對資料控制者發出「資訊請求通知」，要求資料控制者向資訊委員提交指明之特定資訊[170]，並得於資訊請求通知中指定資料提交之形式及提交之期間或日期及地點[171]。

資訊請求通知之內容應包含下列事項[172]：

1、在資訊委員接受評估請求的情況，資訊請求通知之內容應包含資訊委員接受他人請求對資料控制者特定的處理個資行為作出評估的聲明。

---

169 UK, Data Protection Act, Section42(4), "Where the Commissioner has received a request under this section he shall notify the person who made the request—(a)whether he has made an assessment as a result of the request, and(b)to the extent that he considers appropriate, having regard in particular to any exemption from section 7 applying in relation to the personal data concerned, of any view formed or action taken as a result of the request".

170 UK, Data Protection Act, Section43(1), "If the Commissioner—(a)has received a request under section 42 in respect of any processing of personal data, or(b)reasonably requires any information for the purpose of determining whether the data controller has complied or is complying with the data protection principles,he may serve the data controller with a notice (in this Act referred to as "an information notice") requiring the data controller, to furnish the Commissioner with specified information relating to the request or to compliance with the principles".

171 UK, Data Protection Act, Section43(1B), "The Commissioner may also specify in the information notice— (a)the form in which the information must be furnished; (b)the period within which, or the time and place at which, the information must be furnished".

172 UK, Data Protection Act, Section43(2), "An information notice must contain—(a)in a case falling within subsection (1)(a), a statement that the Commissioner has received a request under section 42 in relation to the specified processing, or(b)in a case falling within subsection (1)(b), a statement that the Commissioner regards the specified information as relevant for the purpose of determining whether the data controller has complied, or is complying, with the data protection principles and his reasons for regarding it as relevant for that purpose".

2、在資訊委員為認定資料控制者是否已遵循或正在遵循個資保護原則而須合理要求資料控制者提供資訊的情況，資訊請求通知之內容應包含資訊委員認為哪些資訊與前述目的相關及其理由之聲明。

3、資料控制者得依法聲明不服之權利[173]。

又資訊請求通知要求資料控制者提交資訊之期間不得截止於資料控制者仍得聲明不服之期間，或要求提交之日期不得落於資料控制者仍得聲明不服之期間；且如資料控制者依法聲明不服時，在判決作出或撤回聲明前，均無須提交任何資訊[174]。但如資訊委員有理由因特殊情況認為要求資料控制者提交資訊具急迫性時，得在資訊請求通知中敘明該情形並附理由後要求資料控制者即時（但不得少於資訊請求通知送達日起算７日）遵照辦理[175]。

(五) 推廣優良實務及制定實務指引

資訊委員有義務促使資料控制者遵守優良實務[176]及個

---

[173] UK, Data Protection Act, Section43(3), "An information notice must also contain particulars of the rights of appeal conferred by section 48".

[174] UK, Data Protection Act, Section43(4), "Subject to subsection (5), a period specified in an information notice under subsection (1B)(b) must not end, and a time so specified must not fall, before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the information need not be furnished pending the determination or withdrawal of the appeal".

[175] UK, Data Protection Act, Section43(5), "If by reason of special circumstances the Commissioner considers that the information is required as a matter of urgency, he may include in the notice a statement to that effect and a statement of his reasons for reaching that conclusion; and in that event subsection (4) shall not apply, but the notice shall not require the information to be furnished before the end of the period of seven days beginning with the day on which the notice is served".

[176] 指資訊委員認為足以保障資料當事人等利益且包含但不限於符合個人資料保護法規範的處理個資行為。UK, Data Protection Act, Section51(9), "“good practice” means such practice in the processing of personal data as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, and includes (but is not limited to) compliance with the requirements of this Act".

人資料保護法的各項規定[177]，並應依其認為適當之形式及方式推廣有利於公眾的個人資料保護法因應措施、優良實務及其他與其職權範圍有關之事務，且得就前述事務向任何人提供建議[178]。

資訊委員應依內閣大臣之命令[179]，或自行認為合適時，在適當徵詢商業團體（包含任何代表資料控制者之主體[180]）、資料當事人或其代理人之意見後，制定並宣傳適當的實務指引（code of practice）以作為優良實務的準則[181]。

資訊委員亦應在認為適當時，鼓勵商業團體制定並向其成員宣傳實務指引，且如任何商業團體向資訊委員提出其制定之實務指引尋求建議時，資訊委員應在審視指引內容並適當徵詢資料當事人或其代理人之意見後，將其認定該指引是否遵循優良實務之判斷通知該商業團體[182]。

---

177 UK, Data Protection Act, Section51(1), "It shall be the duty of the Commissioner to promote the following of good practice by data controllers and, in particular, so to perform his functions under this Act as to promote the observance of the requirements of this Act by data controllers".

178 UK, Data Protection Act, Section51(2), "The Commissioner shall arrange for the dissemination in such form and manner as he considers appropriate of such information as it may appear to him expedient to give to the public about the operation of this Act, about good practice, and about other matters within the scope of his functions under this Act, and may give advice to any person as to any of those matters".

179 該命令應描述所要求制定之實務指引涉及的個人資料及處理行為，亦可描述該實務指引涉及的自然人或自然人身分種類。UK, Data Protection Act, Section51(5), " An order under subsection (3) shall describe the personal data or processing to which the code of practice is to relate, and may also describe the persons or classes of persons to whom it is to relate".

180 UK, Data Protection Act, Section51(9), " “trade association” includes any body representing data controllers".

181 UK, Data Protection Act, Section51(3), "Where—(a)the Secretary of Stateso directs by order, or(b)the Commissioner considers it appropriate to do so,the Commissioner shall, after such consultation with trade associations, data subjects or persons representing data subjects as appears to him to be appropriate, prepare and disseminate to such persons as he considers appropriate codes of practice for guidance as to good practice".

182 UK, Data Protection Act, Section51(4), "The Commissioner shall also—(a)where he considers it appropriate to do so, encourage trade associations to prepare, and to disseminate to their members, such codes of practice, and(b)where any trade association submits a code of practice to him for his

(六) 遵循性評估

資訊委員得經資料控制者同意，評估其處理個資之行為是否遵循優良實務，並應將評估結果通知資料控制者[183]。

(七) 報告義務

資訊委員應每年將其執行職權之內容製成業務報告提交兩議院，亦得不定期向兩議院提交其認為適當之職務內容報告。又如內閣大臣命令資訊委員制定實務指引時，資訊委員應將其制定之實務指引提交兩議院，但該指引已包含於前述報告者，不在此限[184]。

(八) 國際合作

資訊委員為英國依歐盟個人資料自動化處理保護公約[185]第 13 條指派的主管機關，亦為英國依歐盟個人資料保護指令[186]及刑事警務及司法合作之資料保護框架第 2008/977/JHA 框架決定[187]規範之主管機關[188]。

---

consideration, consider the code and, after such consultation with data subjects or persons representing data subjects as appears to him to be appropriate, notify the trade association whether in his opinion the code promotes the following of good practice".

183 UK, Data Protection Act, Section51(7), "The Commissioner may, with the consent of the data controller, assess any processing of personal data for the following of good practice and shall inform the data controller of the results of the assessment".

184 UK, Data Protection Act, Section52, "(1)The Commissioner shall lay annually before each House of Parliament a general report on the exercise of his functions under this Act.(2)The Commissioner may from time to time lay before each House of Parliament such other reports with respect to those functions as he thinks fit.(3)The Commissioner shall lay before each House of Parliament any code of practice prepared under section 51(3) for complying with a direction of the Secretary of State , unless the code is included in any report laid under subsection (1) or (2)".

185 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

186 Data Protection Directive.

187 Council Framework Decision 2008/977/ JHA of 27th November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

188 UK, Data Protection Act, Section54(1), " The Commissioner—(a)shall continue to be the designated authority in the United Kingdom for the purposes of Article 13 of the Convention,

(九) 調查海外資訊系統

資訊委員有權調查申根區資訊系統、歐洲刑警組織資訊系統、海關資訊系統中的個人資料紀錄[189]，以評估現在或將來的個資處理行為是否符合個人資料保護法規定[190]，但在執行調查權前，資訊委員應以書面通知該資料控制者[191]，惟資訊委員認有急迫情形者，不在此限[192]。前述調查權內容包含檢查、操作或測試用以處理個人資料之設備[193]。

任何刻意阻礙前述調查權之行使或無合理理由拒絕協助合理調查之人均應承擔刑事責任[194]。

(十) 處罰

任何人未能遵守執行通知或資訊請求通知之要求，將承擔刑事責任[195]，但該人得舉證已盡一切努力遵循要求[196]；又該人若對資訊請求通知基於故意或重大過失而就重要事

---

and(b)shall be the supervisory authority in the United Kingdom for the purposes of the Data Protection Directive and the Data Protection Framework Decision".

189 UK, Data Protection Act, Section54A(1), "The Commissioner may inspect any personal data recorded in—(a)the Schengen information system,(b)the Europol information system,(c)the Customs information system".

190 UK, Data Protection Act, Section54A(2), "The power conferred by subsection (1) is exercisable only for the purpose of assessing whether or not any processing of the data has been or is being carried out in compliance with this Act".

191 UK, Data Protection Act, Section54A(4), "Before exercising the power, the Commissioner must give notice in writing of his intention to do so to the data controller".

192 UK, Data Protection Act, Section54A(5), "But subsection (4) does not apply if the Commissioner considers that the case is one of urgency".

193 UK, Data Protection Act, Section54A(3), "The power includes power to inspect, operate and test equipment which is used for the processing of personal data".

194 UK, Data Protection Act, Section54A(6), "Any person who—(a)intentionally obstructs a person exercising the power conferred by subsection (1), or(b)fails without reasonable excuse to give any person exercising the power any assistance he may reasonably require,is guilty of an offence".

195 UK, Data Protection Act, Section47(1), "A person who fails to comply with an enforcement notice, an information notice or a special information notice is guilty of an offence".

196 UK, Data Protection Act, Section47(3), "It is a defence for a person charged with an offence under subsection (1) to prove that he exercised all due diligence to comply with the notice in question".

項提出虛假資訊者，亦視為犯罪行為[197]。

此外，資訊委員亦得就其調查結果，對資料控制者科處罰款[198]。

[197] UK, Data Protection Act, Section47(2), "A person who, in purported compliance with an information notice or a special information notice—(a)makes a statement which he knows to be false in a material respect, or(b)recklessly makes a statement which is false in a material respect,is guilty of an offence".

[198] UK, Data Protection Act, Section55A(1), "The Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that— (a)there has been a serious contravention of section 4(4) by the data controller, (b)the contravention was of a kind likely to cause substantial damage or substantial distress, and (c)subsection (2) or (3) applies".

第三節　加拿大—隱私委員辦公室（OPC）

一、概述

加拿大為聯邦制國家，於各省設有個別個資或隱私保護專責機關，例如亞伯達資訊及隱私委員、英屬哥倫比亞資訊及隱私委員、曼尼托巴監察使、新布倫瑞克監察使、紐芬蘭與拉布拉多資訊及隱私委員辦公室、西北區資訊及隱私委員、新斯科舍資訊自由及隱私保護審查辦公室、努納福特資訊及隱私委員、安大略資訊及隱私委員、魁北克資訊近用委員會、薩斯喀徹溫資訊及隱私委員，分別掌管個資與隱私保護相關法律。惟本研究聚焦國家級個資或隱私保護專責機關，是僅以加拿大隱私委員辦公室作為研究對象。

加拿大隱私委員辦公室（Office of the Privacy Commissioner of Canada，以下簡稱 OPC）為一對加拿大國會負責的獨立機關，職司《隱私法（Privacy Act）》及《個人資訊保護及電子文件法（Personal Information Protection and Electronic Documents Act）》的任務執行與法規推廣。除在魁北克省加蒂諾市（Gatineau）的總部外，亦在多倫多（Toronto）、安大略（Ontario）設有地區辦公室[199]。

隨著《隱私法》於 1983 年公告，OPC 亦在該年成立，負責執行《隱私法》規管加拿大公務機關對於個人資訊的各項規範；後於 2001 年，規管加拿大非公務機關的《個人資訊保護及電子文件法》通過，OPC 的任務範圍擴張至監管該法的落實。

[199] 見 https://www.priv.gc.ca/en/about-the-opc/，最後到訪日為 106 年 7 月 27 日。

加拿大於《隱私法》第 53 條第 1 項明定由加拿大總督（Governor in Council）請示國會上下議院各政黨領袖意見並經上下議院同意後，指派專人擔任「隱私委員（Privacy Commissioner）」一職[200]，並於該條設立各項隱私委員及 OPC 的組織規範。

二、監管對象與主管法規

加拿大隱私委員辦公室主管《隱私法》及《個人資訊保護及電子文件法》，並依兩法律分別監管公務機關與非公務機關，並得依特定事件的調查結果向法院聲請進入司法程序。

三、組織規範

(一) 地位與兼職禁止

隱私委員之地位等同加拿大政府組織中的副部長（deputy head of a department），並應專責執行《隱私法》及其他相關法案之任務，不得擔任政府或民間機構之有給職[201]。

(二) 任免及代理

隱私委員由加拿大總督指派，一任期為 7 年，但於任期中可隨時由總督依上下議院的決定解任[202]。任期屆滿後得

---

[200] Canada, Privacy Act, Section53(1), "The Governor in Council shall, by commission under the Great Seal, appoint a Privacy Commissioner after consultation with the leader of every recognized party in the Senate and House of Commons and approval of the appointment by resolution of the Senate and House of Commons".

[201] Canada, Privacy Act, Section54(1), "The Privacy Commissioner shall rank as and have all the powers of a deputy head of a department, shall engage exclusively in the duties of the office of Privacy Commissioner under this Act or any other Act of Parliament and shall not hold any other office under Her Majesty for reward or engage in any other employment for reward".

[202] Canada, Privacy Act, Section53(2), "Subject to this section, the Privacy Commissioner holds office

繼續連任，但任期不得超過 7 年，其後亦同[203]。

如隱私委員缺位或無法執行職務時，總督得指派具備適當條件之人暫代隱私委員職務，但不得超過 6 個月。該臨時隱私委員亦得受領薪資或其他由總督決定之報酬[204]。

又總督得指派加拿大《資訊應用法（Access to Information Act）》中的「資訊委員（Information Commissioner）」作為隱私委員[205]。

(三) 薪俸

隱私委員之薪水應與加拿大聯邦法院的法官相同（最高法院首席大法官除外），並有權受領因執行職務所合理支出之旅費或其他經費開銷[206]。但如隱私委員即為加拿大《資訊應用法》下的資訊委員時，僅得受領資訊委員之薪資[207]。

此外，隱私委員亦視為受公務機關僱用而適用加拿大

---

during good behaviour for a term of seven years, but may be removed for cause by the Governor in Council at any time on address of the Senate and House of Commons".

[203] Canada, Privacy Act, Section53(3), "The Privacy Commissioner, on the expiration of a first or any subsequent term of office, is eligible to be re-appointed for a further term not exceeding seven years".

[204] Canada, Privacy Act, Section53(4), "In the event of the absence or incapacity of the Privacy Commissioner, or if that office is vacant, the Governor in Council may appoint any qualified person to hold that office in the interim for a term not exceeding six months, and that person shall, while holding office, be paid the salary or other remuneration and expenses that may be fixed by the Governor in Council".

[205] Canada, Privacy Act, Section55(1), " The Governor in Council may appoint as Privacy Commissioner under section 53 the Information Commissioner appointed under the Access to Information Act".

[206] Canada, Privacy Act, Section54(2), "The Privacy Commissioner shall be paid a salary equal to the salary of a judge of the Federal Court, other than the Chief Justice, and is entitled to be paid reasonable travel and living expenses incurred in the performance of duties under this Act or any other Act of Parliament".

[207] Canada, Privacy Act, Section55(2), "In the event that the Information Commissioner is appointed in accordance with subsection (1) as Privacy Commissioner, the Privacy Commissioner shall, notwithstanding subsection 54(2), be paid the salary of the Information Commissioner but not the salary of the Privacy Commissioner".

《公務人員補償法（Government Employees Compensation Act）》及《航空法（Aeronautics Act）》下的公務人員補償規定[208]。

(四) 助理隱私委員與團隊

總督得依隱私委員的推薦，指派一位以上的助理隱私委員（Assistant Privacy Commissioner）[209]，任期不得超過5年[210]，期滿後得繼續連任，但任期仍不得超過5年，其後亦同[211]。

助理隱私委員應專職擔任其職位以執行隱私委員授權之職務，不得擔任政府或民間機構之有給職[212]，但有權受領由總督決定之薪資及隱私委員認為合理的執行職務之旅費與其他經費開銷[213]。

此外，助理隱私委員亦視為受公務機關僱用而適用加拿大《公務人員補償法》及《航空法》下的公務人員補償

---

[208] Canada, Privacy Act, Section54(4), "The Privacy Commissioner is deemed to be employed in the public service of Canada for the purposes of the Government Employees Compensation Act and any regulations made under section 9 of the Aeronautics Act".

[209] Canada, Privacy Act, Section56(1), "The Governor in Council may, on the recommendation of the Privacy Commissioner, appoint one or more Assistant Privacy Commissioners".

[210] Canada, Privacy Act, Section56(2), "Subject to this section, an Assistant Privacy Commissioner holds office during good behaviour for a term not exceeding five years".

[211] Canada, Privacy Act, Section56(3), "An Assistant Privacy Commissioner, on the expiration of a first or any subsequent term of office, is eligible to be re-appointed for a further term not exceeding five years".

[212] Canada, Privacy Act, Section57(1), "An Assistant Privacy Commissioner shall engage exclusively in such duties or functions of the office of the Privacy Commissioner under this Act or any other Act of Parliament as are delegated by the Privacy Commissioner to that Assistant Privacy Commissioner and shall not hold any other office under Her Majesty for reward or engage in any other employment for reward".

[213] Canada, Privacy Act, Section57(2), "An Assistant Privacy Commissioner is entitled to be paid a salary to be fixed by the Governor in Council and such travel and living expenses incurred in the performance of duties under this Act or any other Act of Parliament as the Privacy Commissioner considers reasonable".

規定[214]。

又隱私委員得依加拿大《文官雇用法（Public Service Employment Act）》任命其認為執行職務所須的官員（officer）及僱員（employee）[215]，亦得就執行任務所需的技術或其他特別事項聘僱臨時人員，且在經加拿大國庫委員會（Treasury Board）許可後決定給付予該人員的酬勞及經費開銷[216]。

(五) 行政委託

隱私委員得授權任何人在授權範圍的限制內行使其權力及執行其任務，但下列職權不在此限[217]：

1、再授權之權力（但得授予助理資訊委員再授權之權力）。

2、《隱私法》第 38 條及第 39 條的年度報告及特別報告義務。

---

[214] Canada, Privacy Act, Section57(4), "An Assistant Privacy Commissioner is deemed to be employed in the public service of Canada for the purposes of the Government Employees Compensation Act and any regulations made under section 9 of the Aeronautics Act".

[215] Canada, Privacy Act, Section58(1), "Such officers and employees as are necessary to enable the Privacy Commissioner to perform the duties and functions of the Commissioner under this Act or any other Act of Parliament shall be appointed in accordance with the Public Service Employment Act".

[216] Canada, Privacy Act, Section58(2), "The Privacy Commissioner may engage on a temporary basis the services of persons having technical or specialized knowledge of any matter relating to the work of the Commissioner to advise and assist the Commissioner in the performance of the duties and functions of the Commissioner under this Act or any other Act of Parliament and, with the approval of the Treasury Board, may fix and pay the remuneration and expenses of such persons".

[217] Canada, Privacy Act, Section59(1), " Subject to subsection (2), the Privacy Commissioner may authorize any person to exercise or perform, subject to such restrictions or limitations as the Commissioner may specify, any of the powers, duties or functions of the Commissioner under this Act except(a) in any case other than a delegation to an Assistant Privacy Commissioner, the power to delegate under this section; and (b) in any case, the powers, duties or functions set out in sections 38 and 39".

3、因公務機關拒絕提供牽涉國際事務或國家安全的個人資訊予資料當事人，經申訴而發起的調查（授權予助理資訊委員除外，但助理資訊委員不得再授權）。但經隱私委員特別指派不超過4位官員或僱員執行該調查者，不在此限[218]。

4、對於總督因涉及國際事務、國家安全或法律執行而指定不開放存取之公務機關個人資訊庫（可拒絕資料當事人存取其個人資訊）所發起之調查（授權予助理資訊委員除外，但助理資訊委員不得再授權）。但經隱私委員特別指派不超過4位官員或僱員執行該調查者，不在此限[219]。

助理隱私委員得再授權任何人於再授權範圍的限制內行使其獲隱私委員授權之權力及執行其獲隱私委員授權之任務[220]。

(六) 組織架構

---

[218] Canada, Privacy Act, Section59(2)(a), "The Privacy Commissioner may not, nor may an Assistant Privacy Commissioner, delegate(a) the investigation of any complaint resulting from a refusal by the head of a government institution to disclose personal information by reason of paragraph 19(1)(a) or (b) or section 21except to one of a maximum of four officers or employees of the Commissioner specifically designated by the Commissioner for the purpose of conducting those investigations".

[219] Canada, Privacy Act, Section59(2)(b), "The Privacy Commissioner may not, nor may an Assistant Privacy Commissioner, delegate ... (b) the investigation under section 36 of files contained in a personal information bank designated under section 18 as an exempt bank on the basis of personal information described in section 21except to one of a maximum of four officers or employees of the Commissioner specifically designated by the Commissioner for the purpose of conducting those investigations".

[220] Canada, Privacy Act, Section59(3), "An Assistant Privacy Commissioner may authorize any person to exercise or perform, subject to such restrictions or limitations as the Assistant Privacy Commissioner may specify, any of the powers, duties or functions of the Privacy Commissioner under this Act that the Assistant Privacy Commissioner is authorized by the Privacy Commissioner to exercise or perform".

現行 OPC 的組織架構除隱私委員外，設有下列各單位[221]：

1、 隱私法調查部（Privacy Act Investigations Branch）

2、 個人資訊及電子文件保護法調查部（PIPEDA Investigations Branch）

3、 稽核與審查部（Audit and Review Branch）

4、 推廣宣傳部（Communications Branch）

5、 法律服務、政策、研究與技術分析部（Legal Services, Policy, Research and Technology Analysis Branch）

6、 行政管理部（Corporate Services Branch）

四、《隱私法》規範之法定職務

(一) 受理、發起投訴與調查投訴

1、受理、發起投訴

依《隱私法》規定，有下列情形之一時，隱私委員應受理並調查投訴人對公務機關有關個人資訊之投訴[222]，投訴人授權他人提出投訴者亦同[223]。除隱私委員另

---

[221] 見 https://www.priv.gc.ca/en/about-the-opc/who-we-are/organizational-structure/，最後到訪為 106 年 8 月 1 日。

[222] Canada, Privacy Act, Section29(1), "Subject to this Act, the Privacy Commissioner shall receive and investigate complaints (a) from individuals who allege that personal information about themselves held by a government institution has been used or disclosed otherwise than in accordance with section 7 or 8; (b) from individuals who have been refused access to personal information requested under subsection 12(1); (c) from individuals who allege that they are not being accorded the rights to which they are entitled under subsection 12(2) or that corrections of personal information requested under paragraph 12(2)(a) are being refused without justification; (d) from individuals who have requested access to personal information in respect of which a time limit

有授權外，該投訴應以書面為之[224]：

(1) 資料當事人宣稱保有其個人資訊的公務機關違法利用、揭露其個人資訊。

(2) 資料當事人遭公務機關拒絕其依法接取（access to）其個人資訊。

(3) 資料當事人宣稱公務機關未依法按其請求更正個人資訊或未註明更正請求遭拒之情事，或其更正請求遭公務機關無正當理由拒絕。

(4) 資料當事人認為公務機關對其接取個人資訊之請求無合理理由延長准駁決定期間。

(5) 公務機關對資料當事人請求接取之個人資訊未依法以官方語言提供。

(6) 公務機關未依具有感知障礙之資料當事人依法請求提供替代形式之個人資訊。

---

has been extended pursuant to section 15 where they consider the extension unreasonable; (e) from individuals who have not been given access to personal information in the official language requested by the individuals under subsection 17(2); (e.1) from individuals who have not been given access to personal information in an alternative format pursuant to a request made under subsection 17(3); (f) from individuals who have been required to pay a fee that they consider inappropriate; (g) in respect of the index referred to in subsection 11(1); or (h) in respect of any other matter relating to (i) the collection, retention or disposal of personal information by a government institution, (ii) the use or disclosure of personal information under the control of a government institution, or (iii) requesting or obtaining access under subsection 12(1) to personal information".

223 Canada, Privacy Act, Section29(2), "Nothing in this Act precludes the Privacy Commissioner from receiving and investigating complaints of a nature described in subsection (1) that are submitted by a person authorized by the complainant to act on behalf of the complainant, and a reference to a complainant in any other section includes a reference to a person so authorized".

224 Canada, Privacy Act, Section30, "A complaint under this Act shall be made to the Privacy Commissioner in writing unless the Commissioner authorizes otherwise".

(7) 資料當事人認其遭要求支付不適當的費用。

(8) 關於公務機關個人資訊索引之事項。

(9) 其他關於下列情形之事項：

A. 公務機關對個人資訊之蒐集、保存、處置。

B. 公務機關對個人資訊之利用、揭露。

C. 請求或獲准存取個人資訊。

此外，隱私委員如依合理根據而認有調查之必要，亦得自行就《隱私法》規定之事項發起投訴[225]。

2、調查投訴事項

隱私委員在調查投訴事項之前，應通知受調查公務機關之首長該調查的意圖及投訴要旨[226]。

投訴人或受調查公務機關之首長有權在調查程序中陳述意見，但任何人均無權要求於他人陳述時在場，亦不得要求獲知他人陳述之內容或對他人之陳述發表評論[227]。

---

[225] Canada, Privacy Act, Section29(3), " Where the Privacy Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Act, the Commissioner may initiate a complaint in respect thereof".

[226] Canada, Privacy Act, Section31, "Before commencing an investigation of a complaint under this Act, the Privacy Commissioner shall notify the head of the government institution concerned of the intention to carry out the investigation and shall inform the head of the institution of the substance of the complaint".

[227] Canada, Privacy Act, Section33(2), "In the course of an investigation of a complaint under this Act by the Privacy Commissioner, the person who made the complaint and the head of the government institution concerned shall be given an opportunity to make representations to the Commissioner, but no one is entitled as of right to be present during, to have access to or to comment on representations made to the Commissioner by any other person".

隱私委員在依《隱私法》對公務機關執行調查時，得行使下列權力[228]：

(1) 以與高等法院作成紀錄相同之方式及範圍，傳喚人員出席調查程序並強制其宣誓（類似我國之具結）後提出隱私委員認為係完成調查所須的口頭或書面證據，或製作文物。

(2) 主持宣誓。

(3) 接受經宣誓而提出的證據或其他資訊；或不論是否得依法提出於法院，但隱私委員認為適當的證據或其他資訊。

(4) 為確認安全條件而進入任何公務機關之處所。

(5) 在公務機關之處所內私下詢問任何人員，或以隱私委員認為合適的其他方式完成詢問。

(6) 對在公務機關之處所內與調查事項有關的文書或記錄執行檢查、獲得複本或摘錄內容。

---

[228] Canada, Privacy Act, Section34(1), "The Privacy Commissioner has, in relation to the carrying out of the investigation of any complaint under this Act, power (a) to summon and enforce the appearance of persons before the Privacy Commissioner and compel them to give oral or written evidence on oath and to produce such documents and things as the Commissioner deems requisite to the full investigation and consideration of the complaint, in the same manner and to the same extent as a superior court of record; (b) to administer oaths; (c) to receive and accept such evidence and other information, whether on oath or by affidavit or otherwise, as the Privacy Commissioner sees fit, whether or not the evidence or information is or would be admissible in a court of law; (d) to enter any premises occupied by any government institution on satisfying any security requirements of the institution relating to the premises; (e) to converse in private with any person in any premises entered pursuant to paragraph (d) and otherwise carry out therein such inquiries within the authority of the Privacy Commissioner under this Act as the Commissioner sees fit; and (f) to examine or obtain copies of or extracts from books or other records found in any premises entered pursuant to paragraph (d) containing any matter relevant to the investigation".

無論其他法律如何規定，隱私委員均得於調查投訴事項時，檢查受該公務機關控管而以任何形式存在的任何資訊，此權力不因任何理由而受阻礙。但依《隱私法》第 70 條第 1 項豁免適用《隱私法》之加拿大樞密院（Queen's Privy Council for Canada）的機密資訊不在此限[229]。

3、文物歸還

任何人或公務機關均得要求隱私委員於 10 日內歸還因調查投訴事項而取得之文物，但隱私委員有權為調查投訴事項而再次要求提出[230]。

隱私委員依投訴而對公務機關執行之任何調查均不應公開[231]。

4、提出調查結果與建議

如隱私委員在調查投訴事項後認為該投訴有理由，即應向受調查之公務機關首長就下列事項提出報告[232]：

---

[229] Canada, Privacy Act, Section34(2), "Notwithstanding any other Act of Parliament or any privilege under the law of evidence, the Privacy Commissioner may, during the investigation of any complaint under this Act, examine any information recorded in any form under the control of a government institution, other than a confidence of the Queen's Privy Council for Canada to which subsection 70(1) applies, and no information that the Commissioner may examine under this subsection may be withheld from the Commissioner on any grounds".

[230] Canada, Privacy Act, Section34(5), "Any document or thing produced pursuant to this section by any person or government institution shall be returned by the Privacy Commissioner within ten days after a request is made to the Commissioner by that person or government institution, but nothing in this subsection precludes the Commissioner from again requiring its production in accordance with this section".

[231] Canada, Privacy Act, Section33(1), "Every investigation of a complaint under this Act by the Privacy Commissioner shall be conducted in private".

[232] Canada, Privacy Act, Section35(1), "If, on investigating a complaint under this Act in respect of

(1) 該調查之發現及隱私委員認為適當的任何建議。

(2) 如適當的話，要求該公務機關於期限內回覆隱私委員其已採取或將採取何種行為以遵守隱私委員給予之建議，或不採取任何行為之理由。

隱私委員亦應將調查投訴結果向投訴人提出報告，但如隱私委員已對受調查之公務機關限期回覆改善情況時，應於該期限屆至始向投訴人提出報告[233]。

若受調查之公務機關未於隱私委員限定之期間回覆改善情況，或隱私委員認定其回覆將採取之行為係不足夠、不適當，或無法即時改善時，隱私委員應在對投訴人提出之報告中告知該情事，並得於報告中包含隱私委員認為合適的評論[234]。

如受調查公務機關之首長給予隱私委員之回覆內容是同意投訴人取得其個人資訊時，應一併於回覆時即讓投訴人取得其個人資訊[235]。

---

personal information, the Privacy Commissioner finds that the complaint is well-founded, the Commissioner shall provide the head of the government institution that has control of the personal information with a report containing (a) the findings of the investigation and any recommendations that the Commissioner considers appropriate; and (b) where appropriate, a request that, within a time specified therein, notice be given to the Commissioner of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken".

[233] Canada, Privacy Act, Section35(2), "The Privacy Commissioner shall, after investigating a complaint under this Act, report to the complainant the results of the investigation, but where a notice has been requested under paragraph (1)(b) no report shall be made under this subsection until the expiration of the time within which the notice is to be given to the Commissioner".

[234] Canada, Privacy Act, Section35(3), "Where a notice has been requested under paragraph (1)(b) but no such notice is received by the Commissioner within the time specified therefor or the action described in the notice is, in the opinion of the Commissioner, inadequate or inappropriate or will not be taken in a reasonable time, the Commissioner shall so advise the complainant in his report under subsection (2) and may include in the report such comments on the matter as he thinks fit".

[235] Canada, Privacy Act, Section35(4), "Where, pursuant to a request under paragraph (1)(b), the head

又若調查投訴之結果為仍拒絕投訴人取得其個人資訊時，隱私委員應告知投訴人其有權向法院聲請審查該經投訴而調查之事項[236]。

(二) 專業研究

隱私委員應依司法部長（Minister of Justice）之交辦就下列事項進行專業研究，並隨時向司法部長提出報告[237]：

1、與個人隱私有關。

2、資料當事人在《隱私法》規範下就其個人資訊享有權利之範圍。

3、有關除公務機關外，其他據法源依據之個人或機關所蒐集、保存、處置、使用、揭露個人資訊之事項。

司法部長應於接受隱私委員提出專業研究報告日後 15 天內，將該報告交付任一在會期中的議院[238]。

---

of a government institution gives notice to the Privacy Commissioner that access to personal information will be given to a complainant, the head of the institution shall give the complainant access to the information forthwith on giving the notice".

[236] Canada, Privacy Act, Section35(5), "Where, following the investigation of a complaint relating to a refusal to give access to personal information under this Act, access is not given to the complainant, the Privacy Commissioner shall inform the complainant that the complainant has the right to apply to the Court for a review of the matter investigated".

[237] Canada, Privacy Act, Section60(1), "The Privacy Commissioner shall carry out or cause to be carried out such studies as may be referred to the Commissioner by the Minister of Justice (a) relating to the privacy of individuals, (b) concerning the extension of the rights to which individuals are entitled under this Act in respect of personal information about themselves, and (c) relating to the collection, retention, disposal, use or disclosure of personal information by persons or bodies, other than government institutions, that come within the legislative authority of Parliament, and the Privacy Commissioner shall report thereon to the Minister of Justice from time to time".

[238] Canada, Privacy Act, Section60(2), "The Minister of Justice shall cause each report by the Privacy Commissioner under subsection (1) to be laid before Parliament on any of the first fifteen days after receipt thereof that either House of Parliament is sitting".

(三) 審查未開放存取之公務機關個人資訊庫

由於依《隱私法》規定，加拿大總督得指定特定與國際事務、國家安全或法律執行有關之公務機關個人資訊庫無須開放存取，即得不提供資料當事人存取其個人資訊[239]，因此《隱私法》亦賦予隱私委員審查權限，規定隱私委員得隨時對未開放存取之公務機關個人資訊庫內的個人資訊檔案執行調查[240]。

如隱私委員於調查後認為存有任何個人資訊檔案不應包含於該未開放存取之公務機關個人資料庫時，應向該管公務機關首長就下列事項提出報告[241]：

1、隱私委員的發現及其認為適當的任何建議。

2、如適當的話，要求該公務機關於期限內回覆隱私委員其已採取或將採取何種行為以遵守隱私委員給予之建議，或不採取任何行為之理由。

上述報告及公務機關之回覆均得記載於隱私委員依

---

239 Canada, Privacy Act, Section18(1), "The Governor in Council may, by order, designate as exempt banks certain personal information banks that contain files all of which consist predominantly of personal information described in section 21 or 22".

240 Canada, Privacy Act, Section36(1), "The Privacy Commissioner may, from time to time at the discretion of the Commissioner, carry out investigations of the files contained in personal information banks designated as exempt banks under section 18".

241 Canada, Privacy Act, Section36(3), "If, following an investigation under subsection (1), the Privacy Commissioner considers that any file contained in a personal information bank should not be contained therein within the terms of the order designating the bank as an exempt bank, the Commissioner shall provide the head of the government institution that has control of the bank with a report containing (a) the findings of the Commissioner and any recommendations that the Commissioner considers appropriate; and (b) where appropriate, a request that, within a time specified therein, notice be given to the Commissioner of any action taken or proposed to be taken to implement the recommendations or reasons why no such action has been or is proposed to be taken".

《隱私法》規定應對國會提出的年度報告或特殊報告中[242]。

又若該公務機關未於隱私委員限定之期間回覆改正情況，或隱私委員認定其回覆將採取之行為係不足夠、不適當，或無法即時改正時，隱私委員得向法院聲請審查該個人資訊檔案[243]。

(四) 審查法律遵循

隱私委員得隨時對公務機關是否遵守《隱私法》第 4 條至第 8 條關於個人資訊之蒐集、保存、正確、處置、利用、揭露等規定執行調查[244]。

如隱私委員於調查後發現該公務機關未遵守前述規定，隱私委員應對該公務機關首長提出報告，內容包含其發現及任何適當之建議[245]。前述報告得記載於隱私委員依《隱私法》規定應對國會提出的年度報告或特殊報告中[246]。

(五) 報告義務

---

[242] Canada, Privacy Act, Section36(4), "Any report made by the Privacy Commissioner under subsection (3), together with any notice given to the Commissioner in response thereto, may be included in a report made pursuant to section 38 or 39".

[243] Canada, Privacy Act, Section36(5), "Where the Privacy Commissioner requests a notice under paragraph (3)(b) in respect of any file contained in a personal information bank designated under section 18 as an exempt bank and no notice is received within the time specified therefor or the action described in the notice is, in the opinion of the Commissioner, inadequate or inappropriate or will not be taken in a reasonable time, the Privacy Commissioner may make an application to the Court under section 43".

[244] Canada, Privacy Act, Section37(1), "The Privacy Commissioner may, from time to time at the discretion of the Commissioner, carry out investigations in respect of personal information under the control of government institutions to ensure compliance with sections 4 to 8".

[245] Canada, Privacy Act, Section37(3), "If, following an investigation under subsection (1), the Privacy Commissioner considers that a government institution has not complied with sections 4 to 8, the Commissioner shall provide the head of the institution with a report containing the findings of the investigation and any recommendations that the Commissioner considers appropriate".

[246] Canada, Privacy Act, Section37(4), "Any report made by the Privacy Commissioner under subsection (3) may be included in a report made pursuant to section 38 or 39".

隱私委員須在每財務年度結束後 3 個月內將記載隱私委員辦公室於該年度內的所有活動之年度報告提出於國會[247]。

隱私委員亦得隨時就其認為與其權力、任務、職權有關且具有緊急性與重要性而不應遲至年度報告始提出之事項製成特殊報告提出於國會[248]。

(六) 處罰

任何人均不得阻礙隱私委員或其委託之人行使《隱私法》下的職權與執行其任務[249]，如有違反，將構成刑事責任，一經定罪可處最高 1000 元加幣罰金[250]。

五、《個人資訊保護及電子文件法》規範之法定職務

(一) 受理、發起投訴與調查投訴

1、受理、發起投訴

資料當事人得因非公務機關違反《個人資訊保護及電子文件法》第 1 部第 1 分部（Part 1, Division 1）關於個人資訊保護之規定或未遵守附表 1（Schedule 1）的

---

247 Canada, Privacy Act, Section38, "The Privacy Commissioner shall, within three months after the termination of each financial year, submit an annual report to Parliament on the activities of the office during that financial year".

248 Canada, Privacy Act, Section39(1), "The Privacy Commissioner may, at any time, make a special report to Parliament referring to and commenting on any matter within the scope of the powers, duties and functions of the Commissioner where, in the opinion of the Commissioner, the matter is of such urgency or importance that a report thereon should not be deferred until the time provided for transmission of the next annual report of the Commissioner under section 38".

249 Canada, Privacy Act, Section68(1), "No person shall obstruct the Privacy Commissioner or any person acting on behalf or under the direction of the Commissioner in the performance of the Commissioner's duties and functions under this Act".

250 Canada, Privacy Act, Section68(2), "Every person who contravenes this section is guilty of an offence and liable on summary conviction to a fine not exceeding one thousand dollars".

各項個資保護原則，向隱私委員以書面提出投訴[251]。但如該投訴係針對非公務機關拒絕資料當事人存取其個人資訊時，資料當事人應於受拒絕之日或非公務機關應答覆准許與否之日屆滿後 6 個月內或隱私委員許可之較長期限內提出投訴[252]。

隱私委員如有合理根據認有應調查之事項時，亦得就該事項自行發起投訴[253]。

無論由投訴人提出投訴或由隱私委員發起投訴，隱私委員均應將遭投訴之事實通知該非公務機關[254]。

2、調查投訴事項

除隱私委員認有下列情形外，隱私委員應對投訴事項執行調查[255]：

(1) 投訴者應先循其他可得之申訴或審查程序救濟。

(2) 該投訴如依加拿大（某省）之法律程序處理更為適

---

[251] Canada, PIPEDA, Section11(1), "An individual may file with the Commissioner a written complaint against an organization for contravening a provision of Division 1 or for not following a recommendation set out in Schedule 1".

[252] Canada, PIPEDA, Section11(3), "A complaint that results from the refusal to grant a request under section 8 must be filed within six months, or any longer period that the Commissioner allows, after the refusal or after the expiry of the time limit for responding to the request, as the case may be".

[253] Canada, PIPEDA, Section11(2), "If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Part, the Commissioner may initiate a complaint in respect of the matter".

[254] Canada, PIPEDA, Section11(4), "The Commissioner shall give notice of a complaint to the organization against which the complaint was made".

[255] Canada, PIPEDA, Section12(1), "The Commissioner shall conduct an investigation in respect of a complaint, unless the Commissioner is of the opinion that (a) the complainant ought first to exhaust grievance or review procedures otherwise reasonably available; (b) the complaint could more appropriately be dealt with, initially or completely, by means of a procedure provided for under the laws of Canada, other than this Part, or the laws of a province; or (c) the complaint was not filed within a reasonable period after the day on which the subject matter of the complaint arose".

當。

(3) 該投訴未於投訴事項發生日後的合理期間內提出。

隱私委員應將不對投訴事項執行調查或不採取行動之決定通知投訴人及該非公務機關，並敘明理由[256]。惟如投訴人提出堅強之理由時，隱私委員得重新考量其不對投訴事項執行調查的決定[257]。

隱私委員在對非公務機關執行投訴事項的調查時，得行使下列權力[258]：

(1) 以與高等法院作成紀錄相同之方式及範圍，傳喚人員出席調查程序並強制其宣誓（類似我國之具結）後提出隱私委員認為係完成調查所須的口頭或書面證據，或製作文物。

(2) 主持宣誓。

---

[256] Canada, PIPEDA, Section12(3), "The Commissioner shall notify the complainant and the organization that the Commissioner will not investigate the complaint or any act alleged in the complaint and give reasons".

[257] Canada, PIPEDA, Section12(4), "The Commissioner may reconsider a decision not to investigate under subsection (1), if the Commissioner is satisfied that the complainant has established that there are compelling reasons to investigate".

[258] Canada, PIPEDA, Section12.1(1), "In the conduct of an investigation of a complaint, the Commissioner may (a) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary to investigate the complaint, in the same manner and to the same extent as a superior court of record; (b) administer oaths; (c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit, whether or not it is or would be admissible in a court of law; (d) at any reasonable time, enter any premises, other than a dwelling-house, occupied by an organization on satisfying any security requirements of the organization relating to the premises; (e) converse in private with any person in any premises entered under paragraph (d) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and (f) examine or obtain copies of or extracts from records found in any premises entered under paragraph (d) that contain any matter relevant to the investigation".

(3) 接受經宣誓而提出的證據或其他資訊；或不論是否得依法提出於法院，但隱私委員認為適當的證據或其他資訊。

(4) 在合理時間內，為確認安全條件而進入該非公務機關之任何處所，但住宅除外。

(5) 在該非公務機關之處所內私下詢問任何人員，或以隱私委員認為合適的其他方式完成詢問。

(6) 對在該非公務機關之處所內與調查事項有關的文書或記錄執行檢查、獲得複本或摘錄內容。

3、爭議解決

隱私委員得嘗試以爭議解決機制處理投訴事項，例如和解或調解[259]。

4、行政委託

隱私委員得將前述調查及爭議解決之權力委託他人執行[260]，但應出具證明予該受託之人，使其在進入任何處所行使權力時，應該處所主管人員之要求提出證明[261]。

5、文物歸還

---

[259] Canada, PIPEDA, Section12.1(2), "The Commissioner may attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation".

[260] Canada, PIPEDA, Section12.1(3), "The Commissioner may delegate any of the powers set out in subsection (1) or (2)".

[261] Canada, PIPEDA, Section12.1(5), "Any person to whom powers set out in subsection (1) are delegated shall be given a certificate of the delegation and the delegate shall produce the certificate, on request, to the person in charge of any premises to be entered under paragraph (1)(d)".

任何人或非公務機關均得要求隱私委員或其委託之人於 10 日內歸還因調查投訴事項而取得之文物，但隱私委員或其委託之人有權為調查投訴事項而再次要求提出[262]。

6、中止調查

若隱私委員認有下列情況時,得中止對投訴事項執行之調查[263]：

(1) 無足夠證據繼續調查。

(2) 該投訴係瑣碎、無謂、煩躁或出於惡意。

(3) 該非公務機關已對該投訴提出公平、合理之回應。

(4) 該事項係針對隱私委員與該非公務機關依《個人資訊保護及電子文件法》第 17.1 條第 1 項作出的法遵協議（Compliance Agreement）。

(5) 該事項業經他案而遭調查中。

(6) 該事項已成為隱私委員提出報告之內容。

---

[262] Canada, PIPEDA, Section12.1(4), "The Commissioner or the delegate shall return to a person or an organization any record or thing that they produced under this section within 10 days after they make a request to the Commissioner or the delegate, but nothing precludes the Commissioner or the delegate from again requiring that the record or thing be produced".

[263] Canada, PIPEDA, Section12.2(1), "The Commissioner may discontinue the investigation of a complaint if the Commissioner is of the opinion that (a) there is insufficient evidence to pursue the investigation; (b) the complaint is trivial, frivolous or vexatious or is made in bad faith; (c) the organization has provided a fair and reasonable response to the complaint; (c.1) the matter is the object of a compliance agreement entered into under subsection 17.1(1); (d) the matter is already the object of an ongoing investigation under this Part; (e) the matter has already been the subject of a report by the Commissioner; (f) any of the circumstances mentioned in paragraph 12(1)(a), (b) or (c) apply; or (g) the matter is being or has already been addressed under a procedure referred to in paragraph 12(1)(a) or (b)".

(7) 存有「投訴者應先循其他可得之申訴或審查程序救濟」、「該投訴如依加拿大（某省）之法律程序處理更為適當」、「該投訴未於投訴事項發生日後的合理期間內提出」之任一情形。

(8) 該事項已經或刻正於其他申訴、審查或法律程序中被提出。

隱私委員應將中止調查之決定及理由告知投訴人及該非公務機關[264]。

7、提出調查報告

隱私委員應於受理投訴或發起投訴之日起一年內，就下列事項作出報告[265]，並即時交付投訴人及該受調查之非公務機關[266]：

(1) 隱私委員的發現與建議。

(2) 雙方達成的任何和解協議。

(3) 如適當的話，要求該非公務機關於期限內回覆隱私委員其已採取或將採取何種行為以遵守隱私委員給予之建議，或不採取任何行為之理由。

---

[264] Canada, PIPEDA, Section12.2(3), "The Commissioner shall notify the complainant and the organization that the investigation has been discontinued and give reasons".

[265] Canada, PIPEDA, Section13(1), "The Commissioner shall, within one year after the day on which a complaint is filed or is initiated by the Commissioner, prepare a report that contains (a) the Commissioner's findings and recommendations; (b) any settlement that was reached by the parties; (c) if appropriate, a request that the organization give the Commissioner, within a specified time, notice of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken; and (d) the recourse, if any, that is available under section 14".

[266] Canada, PIPEDA, Section13(3), "The report shall be sent to the complainant and the organization without delay".

(4)（如有）投訴人得依《個人資訊保護及電子文件法》第 14 條向法院請求之救濟手段。

8、聲請及出席法院聽證

隱私委員得就投訴人之投訴，在提出調查報告或作出中止調查的決定後[267]：

(1) 經投訴人同意而向法院聲請就投訴事項舉行聽證（Hearing）。

(2) 為投訴人之利益出席法院之聽證。

(3) 在法院許可下以任一方之身分出席聽證。

(二) 作成法遵協議

如隱私委員有合理根據相信某非公務機關已經、將要或可能將（故意或過失）違反《個人資訊保護及電子文件法》第 1 部第 1 分部（Part 1, Division 1）關於個人資訊保護之規定或未遵守附表 1（Schedule 1）的各項個資保護原則時，隱私委員得與該非公務機關達成法遵協議（compliance agreement），內容包含任何隱私委員認為必要之條款[268]，以確保其遵循法律規定[269]。但資料當事人仍有權

[267] Canada, PIPEDA, Section15, "The Commissioner may, in respect of a complaint that the Commissioner did not initiate, (a) apply to the Court, within the time limited by section 14, for a hearing in respect of any matter described in that section, if the Commissioner has the consent of the complainant; (b) appear before the Court on behalf of any complainant who has applied for a hearing under section 14; or (c) with leave of the Court, appear as a party to any hearing applied for under section 14".

[268] Canada, PIPEDA, Section17.1(2), "A compliance agreement may contain any terms that the Commissioner considers necessary to ensure compliance with this Part".

[269] Canada, PIPEDA, Section17.1(1), "If the Commissioner believes on reasonable grounds that an organization has committed, is about to commit or is likely to commit an act or omission that could constitute a contravention of a provision of Division 1 or 1.1 or a failure to follow a

依《個人資訊保護及電子文件法》第 14 條規定向法院聲請聽證，且不妨礙該法下的刑事訴追[270]。

在法遵協議作成後，隱私委員就協議中的任何事項[271]：

1、不得向法院聲請舉行聽證。

2、應向法院請求暫停任何隱私委員已聲請關於聽證之行為。

如隱私委員認為該非公務機關確實遵守法遵協議時，應以書面通知該非公務機關，並撤回由資料當事人或隱私委員聲請法院關於舉行聽證之任何行為[272]。

但若隱私委員認為該非公務機關未遵守法遵協議時，除應通知該非公務機關外，隱私委員亦得於該通知送達後一年內或法院許可之較長期間內[273]，向法院聲請[274]：

---

recommendation set out in Schedule 1, the Commissioner may enter into a compliance agreement, aimed at ensuring compliance with this Part, with that organization".

270 Canada, PIPEDA, Section17.1(4), "For greater certainty, a compliance agreement does not preclude (a) an individual from applying for a hearing under section 14; or (b) the prosecution of an offence under the Act".

271 Canada, PIPEDA, Section17.1(3), "When a compliance agreement is entered into, the Commissioner, in respect of any matter covered under the agreement, (a) shall not apply to the Court for a hearing under subsection 14(1) or paragraph 15(a); and (b) shall apply to the court for the suspension of any pending applications that were made by the Commissioner under those provisions".

272 Canada, PIPEDA, Section17.2(1), "If the Commissioner is of the opinion that a compliance agreement has been complied with, the Commissioner shall provide written notice to that effect to the organization and withdraw any applications that were made under subsection 14(1) or paragraph 15(a) in respect of any matter covered under the agreement".

273 Canada, PIPEDA, Section17.2(3), "Despite subsection 14(2), the application shall be made within one year after notification is sent or within any longer period that the Court may, either before or after the expiry of that year, allow".

274 Canada, PIPEDA, Section17.2(2), "If the Commissioner is of the opinion that an organization is not complying with the terms of a compliance agreement, the Commissioner shall notify the organization and may apply to the Court for (a) an order requiring the organization to comply with the terms of the agreement, in addition to any other remedies it may give; or (b) a hearing under subsection 14(1) or paragraph 15(a) or to reinstate proceedings that have been suspended as a result

1、命令該非公務機關遵守法遵協議，及其他補救措施。

2、舉行聽證或繼續進行之前已向法院請求暫停關於聽證之行為。

(三) 稽核

隱私委員如有合理根據認為某非公務機關已違反《個人資訊保護及電子文件法》第 1 部第 1 分部（Part 1, Division 1）關於個人資訊保護之規定或未遵守附表 1（Schedule 1）的各項個資保護原則建議時，得以合理通知後，於合理時間對該非公務機關的個資管理措施執行稽核[275]，並應將稽核報告提供該受稽核之非公務機關，內容應包含稽核發現及隱私委員認為適當之任何建議[276]。

(四) 推廣

隱私委員應以任何適當之方式推廣相關的隱私法規，並應制定、執行資訊推廣措施，以提升公眾對於隱私法規的理解與認知，且應發布任何與個資保護有關之研究，同時應鼓勵非公務機關制定詳細的政策或措施（包含實務指引）以遵循隱私法規[277]。

---

of an application made under paragraph 17.1(3)(b)".

[275] Canada, PIPEDA, Section18(1), "The Commissioner may, on reasonable notice and at any reasonable time, audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization has contravened a provision of Division 1 or 1.1 or is not following a recommendation set out in Schedule 1".

[276] Canada, PIPEDA, Section19(1), "After an audit, the Commissioner shall provide the audited organization with a report that contains the findings of the audit and any recommendations that the Commissioner considers appropriate".

[277] Canada, PIPEDA, Section24, "The Commissioner shall (a) develop and conduct information programs to foster public understanding, and recognition of the purposes, of this Part; (b) undertake and publish research that is related to the protection of personal information, including any such research that is requested by the Minister of Industry; (c) encourage organizations to

(五) 年度報告

隱私委員應於每財務年度結束後 3 個月內，將該年度的法規執行適用情形向國會提出報告[278]。

(六) 處罰

任何阻礙隱私委員或其委託之人行使調查權或執行稽核之人均構成犯罪，一經定罪可處最高 1 萬元加幣罰金（簡易處刑）或最高 10 萬元加幣罰金（通常程序）[279]。

develop detailed policies and practices, including organizational codes of practice, to comply with sections 5 to 10; and (d) promote, by any means that the Commissioner considers appropriate, the purposes of this Part".

[278] Canada, PIPEDA, Section25(1), "The Commissioner shall, within three months after the end of each financial year, submit to Parliament a report concerning the application of this Part, the extent to which the provinces have enacted legislation that is substantially similar to this Part and the application of any such legislation".

[279] Canada, PIPEDA, Section28, "Every person ..... who obstructs the Commissioner or the Commissioner's delegate in the investigation of a complaint or in conducting an audit is guilty of (a) an offence punishable on summary conviction and liable to a fine not exceeding $10,000; or (b) an indictable offence and liable to a fine not exceeding $100,000".

第四節　香港—個人資料私隱專員公署

一、概述

香港個人資料私隱專員公署（以下簡稱公署）成立於 1996 年 8 月 1 日，乃一獨立法定機構，職司監管香港個人資料(私隱）條例（以下簡稱條例）的施行。

條例第 5 條創設「個人資料私隱專員」職位，由行政長官委任一人作為專員[280]，具有起訴與被訴的訴訟能力[281]。

二、監管對象與主管法規

公署僅負責個人資料（私隱）條例的執行實施，未同時監管其他法律；並依條例規定，公務機關及非公務機關均受拘束，並得由公署專員予以處罰。

三、組織規範

(一) 地位

專員除為香港「防止賄賂條例」下的公職人員外，並不具有香港政府的僱員或代理人身分，也不享有香港政府的地位、豁免權或特權[282]。

(二) 任免、禁止兼職與出缺

出任專員之條款與條件由行政長官決定[283]，任期為 5

[280] 香港，個人資料(私隱)條例，第 5 條第(3)款。
[281] 香港，個人資料(私隱)條例，第 5 條第(2)(b)款。
[282] 香港，個人資料(私隱)條例，第 5 條第(8)款、第(9)款。
[283] 香港，個人資料(私隱)條例，第 5 條第(6)(b)款。

年，得再獲委任，但以一期 5 年為限[284]。專員於任期中得隨時以書面通知向行政長官辭職，或因「無能力執行其職位的職能」或「行為不當」而經香港立法會決議由行政長官批准免任[285]。

又專員未經行政長官明確批准不得擔任其他任何有酬職位，亦不得為報酬而從事專員職位以外的任何職業[286]。

而若專員因身故、辭職、遭免任、離開香港或其他理由不能行使職權時，行政長官得以書面委任一人署理專員職位，至行政長官委任新專員或原專員回任[287]，但該署理專員職位之人亦受前述禁止兼職之限制[288]。

(三) 薪酬

專員為有給職，由行政長官決定專員之薪酬[289]，並由專員的「資源」撥付（見下述）[290]。

(四) 職員

專員為執行任務及行使權力，得僱用其認為合適之人（包含技術工作者或專業人士）或以僱用以外之方式聘用其認為適合的技術工作者或專業人士[291]，並決定僱用或聘用

284 香港，個人資料(私隱)條例，第 5 條第(4)款。
285 香港，個人資料(私隱)條例，第 5 條第(5)款。
286 香港，個人資料(私隱)條例，第 6 條。
287 香港，個人資料(私隱)條例，第 7 條第(1)款。
288 香港，個人資料(私隱)條例，第 7 條第(3)款。
289 香港，個人資料(私隱)條例，第 5 條第(6)(a)款。
290 香港，個人資料(私隱)條例，附表 2，第 1 條第(3)(a)款。
291 香港，個人資料(私隱)條例，第 9 條第(1)款。

之條款、條件及薪酬[292]，其薪酬由專員的「資源」撥付（見下述）[293]。

專員可在合適的「規限條款及條件」下，將其任務或權力授權予其僱用或聘用之人，但條例附表 2 或依據條例訂立的規例中有相反規定者，不在此限，且被授權之人不得再授權[294]。

(五) 財務事宜[295]

1、專員資源

專員之資源包含「立法會撥作委員會用途並由政府付予專員的款項」、「由政府以其他方式提供予專員之款項」及「專員所收之餽贈、捐贈、費用、租金、利息及累積收益等所有其他款項及財產」，用以給付專員及專員聘僱用之人的薪酬或其他利益及開銷[296]。

而香港財經事務及庫務局局長得就專員在任何財政年度內可支出的款項提出一般性或具體性的書面指示，要求專員遵守[297]。

2、借款權

香港政制及內地事務局局長經諮詢財經事務及庫務局局長後，可向專員發出一般性或具體書面指示，決

---

[292] 香港，個人資料(私隱)條例，第 9 條第(2)款。
[293] 香港，個人資料(私隱)條例，附表 2，第 1 條第(3)(b)款。
[294] 香港，個人資料(私隱)條例，第 10 條。
[295] 香港，個人資料(私隱)條例，附表 2。
[296] 香港，個人資料(私隱)條例，附表 2，第 1 條第(1)款、第(3)款。
[297] 香港，個人資料(私隱)條例，附表 2，第 1 條第(2)款。

定專員為履行責任及執行任務所需以透支方式借貸款項之額度[298]。專員亦可以透支以外之方式借貸所需款項，但須得到政制及內地事務局局長經諮詢財經事務及庫務局局長後給予之批准[299]。

3、盈餘投資

在得到政制及內地事務局局長經諮詢財經事務及庫務局局長後給予之批准後，專員得將非即時需用之款項用以投資[300]。

4、帳目、審計及年報

專員須將其所有財務往來備妥帳目，並於財政年度屆滿後，在切實可行範圍內儘速製作帳目報表（包含收支結算表及資產負債表），同時委任核數師[301]審計該帳目及帳目報表，再向專員提出報告[302]。

在財政年度屆滿後9個月內或在政務司司長准許的較長期間內，專員須在切實可行的範圍內盡速向政務司司長提交「專員在該年度的事務報告」、「年度帳目報表」及「核數師就該帳目報表作出的報告」，並由政務司司長交由香港立法會[303]。

5、審計審核

---

298 香港，個人資料(私隱)條例，附表2，第2條第(1)款、第(2)款。
299 香港，個人資料(私隱)條例，附表2，第2條第(3)款。
300 香港，個人資料(私隱)條例，附表2，第3條。
301 依香港《專業會計師條例》規定，為機關外部的財務稽核員，須具備香港會計師資格。
302 香港，個人資料(私隱)條例，附表2，第4條第(1)款、第(2)款、第(3)款。
303 香港，個人資料(私隱)條例，附表2，第4條第(4)款。

香港審計署署長得就任何財政年度，對專員在執行任務或行使權力時使用之資源是否合乎經濟原則及效率一事進行審核[304]，並有權在任何合理時間及合理範圍內查閱由專員保管或控制的任何文件，且有權要求持有該文件或對該文件負責之人提出合理的資料及解釋[305]。

6、豁免徵稅

專員得豁免繳交香港稅務條例下的徵稅，但由專員的資源撥付予專員的薪酬、利益與開銷費不在此限[306]。

(六) 組織架構

現行公署的組織架構除個人資料私隱專員及一位副個人資料私隱專員外，設有下列各內部單位：

1、政策及研究部

2、合規部

3、傳訊及教育部

4、法律部（由副私隱專員管轄）

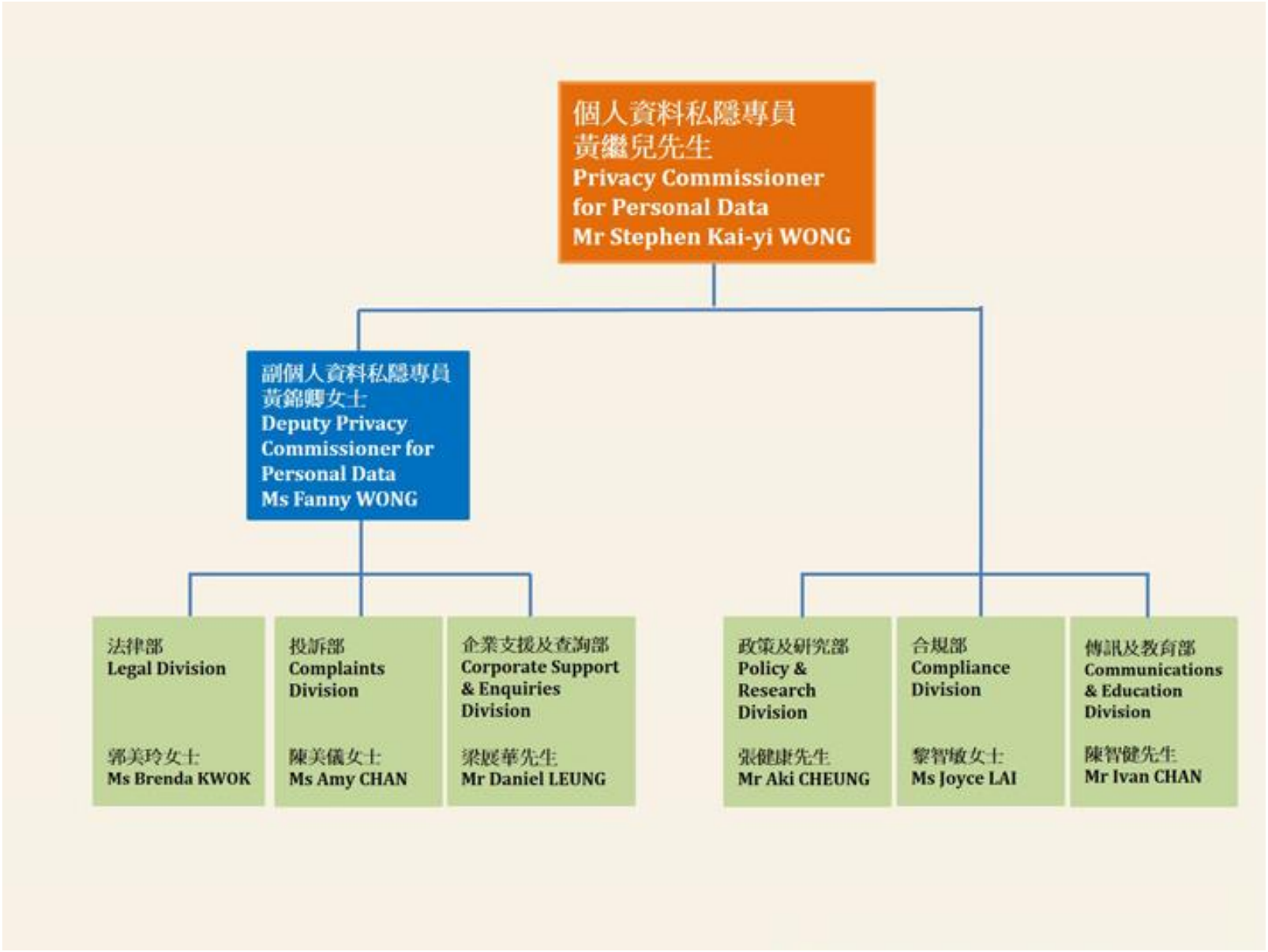
5、投訴部（由副私隱專員管轄）

6、企業支援及查詢部（由副私隱專員管轄）

---

[304] 香港，個人資料(私隱)條例，附表 2，第 5 條第(1)款。
[305] 香港，個人資料(私隱)條例，附表 2，第 5 條第(2)款。
[306] 香港，個人資料(私隱)條例，附表 2，第 6 條。

圖 2 香港個人資料私隱專員公署組織架構圖



四、法定職務

(一) 制定並／或核准實務守則

專員須促進及協助代表資料使用者的團體制定及施行實務守則，以對條例提供指引[307]，即專員可制定並核准適合的實務守則，或核准由他人制定之實務守則[308]（但專員得部分核准[309]），並藉憲報公告及指明生效日期與該守則所針對之條例規定[310]。惟專員有權針對不同的資料使用者就相同或不同的規定制定不同的實務守則[311]。

專員得隨時修訂其制定的實務守則或核准修訂以生效的實務守則[312]，亦可隨時撤回其已核准的實務守則[313]，但須由憲報公告並指明該守則的失效日[314]。

(二) 視察、投訴及調查

1、視察個人資料系統

專員須對屬於政府部門或法人的資料使用者所使用的個人資料系統進行視察[315]，以向特定或特定類別的資料使用者提出建議[316]。

---

[307] 香港，個人資料(私隱)條例，第 8 條第(1)(b)款。
[308] 香港，個人資料(私隱)條例，第 12 條第(1)款。
[309] 香港，個人資料(私隱)條例，第 12 條第(7)款。
[310] 香港，個人資料(私隱)條例，第 12 條第(2)款。
[311] 香港，個人資料(私隱)條例，第 12 條第(10)款。
[312] 香港，個人資料(私隱)條例，第 12 條第(3)款。
[313] 香港，個人資料(私隱)條例，第 12 條第(4)款。
[314] 香港，個人資料(私隱)條例，第 12 條第(5)款。
[315] 香港，個人資料(私隱)條例，第 8 條第(1)(e)款。
[316] 香港，個人資料(私隱)條例，第 36 條。

2、調查投訴及拒絕或終止調查

如專員有合理理由相信資料使用者已經或正在從事有關個人資料且可能違反條例規定之行為時，即可對資料使用者進行調查以確認其行為是否違反條例規定[317]。

除上述情形外，任何人均得就資料使用者所為有關其個人資料且可能違反條例規定之行為向專員投訴，並得要求專員及專員僱用之人提供適當協助以擬訂投訴內容[318]。

專員於收受合法投訴後即應對有關的資料使用者進行調查，以確定在投訴中指明之行為是否違反條例規定[319]。但有下列情形時，專員得拒絕進行或終止由投訴引發的調查[320]：

(1) 投訴人在專員受理投訴之日 2 年前已實際知悉存有該投訴中指明之行為。惟如專員認為在該個案中進行或不終止調查為適當時，不在此限。

(2) 該投訴係由匿名者作出。

(3) 投訴人的身分無法辨識或無法尋獲投訴人。

(4) 投訴人的身分無法辨識或無法尋獲投訴人。

---

317 香港，個人資料(私隱)條例，第 38 條(b)段。
318 香港，個人資料(私隱)條例，第 37 條。
319 香港，個人資料(私隱)條例，第 38 條(a)段。
320 香港，個人資料(私隱)條例，第 39 條第(1)款。

(5) 就該投訴指明之行為，以下狀況均不符合：

A. 在該行為發生時，投訴人居於香港。

B. 在該行為發生時，資料使用者能由香港控制相關個人資料的「收集、持有、處理或使用」，或能從香港行使該控制權。

C. 在該行為發生時，投訴人位於香港。

D. 專員認為該行為可能損害投訴人強制執行在香港獲取或產生的權利或行使在香港獲取或產生的特權。

(6) 專員相信被投訴的資料使用者在專員受理投訴之日前 2 年內，並非是資料使用者。

又專員於考量個案的所有情況後，相信有下列情況時，亦可拒絕進行或終止由投訴引發之調查[321]：

(1) 該投訴或另一性質相似之投訴已在先前引發專員調查，而專員在先前調查後認定並無違反條例規定的情形。

(2) 該投訴指明之行為微不足道。

(3) 該投訴屬瑣屑無聊或無理取鬧，或非真誠提出。

(4) 該投訴指明之行為顯示該投訴的主要標的事宜非關個人資料的隱私。

---

[321] 香港，個人資料(私隱)條例，第 39 條第(2)款。

(5) 其他任何理由可認無必要調查。

若專員拒絕調查投訴事項，應於受理投訴日後 45 天內，在確實可行的範圍內，盡快以書面向投訴人通知拒絕事實及拒絕理由[322]；又若專員係在由投訴引發之調查完成前決定終止該調查，專員亦應在確實可行的範圍內，盡快以書面向投訴人通知該決定及理由[323]。前述書面通知均應載明投訴人得向行政上訴委員會提出上訴[324]。

此外，即便投訴人撤回投訴，但如專員認為進行或繼續進行調查係符合公共利益時，仍可進行調查。在此情況下，該投訴視為未撤回[325]。

3、視察與調查通知

專員在視察或調查前，應將視察或調查之意向以書面通知送達受視察或調查的資料使用者。但專員有合理理由認為事前通知將損害調查之目的者不在此限[326]。

4、強制處分權—為視察個人資料系統而進入處所

專員為視察個人資料系統之目的，得至少在擬視察日 14 天前以書面通知資料使用者「擬進入之處所」及「該通知送達後 14 日屆滿前，不會行使權力」後，於

[322] 香港，個人資料(私隱)條例，第 39 條第(3)款。
[323] 香港，個人資料(私隱)條例，第 39 條第(3A)款。
[324] 香港，個人資料(私隱)條例，第 39 條第(4)款。
[325] 香港，個人資料(私隱)條例，第 40 條。
[326] 香港，個人資料(私隱)條例，第 41 條。

擬視察日進入其內有屬於受視察對象的個人資料系統（全部或部分）之處所進行視察，如該處所非屬住宅，即可在任何合理時間進入，惟若該處所為住宅，則須在該處所居住之任何人（未成年人除外）的同意下始得進入[327]。

但若專員就某處所以某方式行使視察權將對該處所內正在進行之作業構成不當打擾時，專員即不得以該方式就該處所行使視察權[328]。

又在專員行使視察權時，資料使用者須免費提供專員為視察而合理要求的設施及協助[329]。

5、強制處分權—為調查資料使用者行為而進入處所

專員為調查資料使用者行為之目的，得至少在擬調查日 14 天前以書面通知資料使用者「擬進入之處所」及「該通知送達後 14 日屆滿前，不會行使權力」後，進入由資料使用者佔用或其內有資料使用者所使用的個人資料系統（全部或部分）之任何處所進行調查[330]。但如香港裁判官因專員或專員僱用之人經宣示而作之告發，有合理理由相信如專員在行使調查權前先以書面通知，將對調查目的造成重大損害，裁判官得對該處所發出手令(類似搜索票)以免除專員的書面通知義務[331]。

---

327 香港，個人資料(私隱)條例，第 42 條第(1)款、第(3)款。
328 香港，個人資料(私隱)條例，第 42 條第(8)款。
329 香港，個人資料(私隱)條例，第 42 條第(9)款。
330 香港，個人資料(私隱)條例，第 42 條第(2)款、第(3)款。
331 香港，個人資料(私隱)條例，第 42 條第(5)款、第(6)款。

惟如該處所內的任何人質疑專員於該處所行使調查權的權限時，專員即須出示該手令以供該人查閱[332]。

如專員欲進入「住宅」處所行使調查權時，除非專員在依前述規定送達書面通知後 14 天內得到居住該住宅處所之人（未成年人除外）同意，否則專員不得進入該住宅處所行使調查權[333]。但如香港裁判官因專員或專員僱用之人經宣示而作之告發，有合理理由相信如專員因未得同意而無法進入該住宅處所行使調查權，將對調查目的造成重大損害時，裁判官可發出手令以批准專員進入該住宅處所行使調查權[334]。

又若專員就某處所以某方式行使調查察權將對該處所內正在進行之作業構成不當打擾時，專員即不得以該方式就該處所行使調查權[335]；另在專員行使調查權時，資料使用者須免費提供專員為調查而合理要求的設施及協助[336]。

6、強制處分權—文件調閱與陳述意見

專員為調查之目的，得要求其認為合適之人提出合適之資訊、文件或物品，並作出專員認為合適的查訊[337]。如專員認有進行聆訊之必要[338]，則除有下列情形外，聆

[332] 香港，個人資料(私隱)條例，第 42 條第(10)款。
[333] 香港，個人資料(私隱)條例，第 42 條第(4)款。
[334] 香港，個人資料(私隱)條例，第 42 條第(7)款。
[335] 香港，個人資料(私隱)條例，第 42 條第(8)款。
[336] 香港，個人資料(私隱)條例，第 42 條第(9)款。
[337] 香港，個人資料(私隱)條例，第 43 條第(1)款。
[338] 香港，個人資料(私隱)條例，第 43 條第(4)款，「專員不一定要為調查的目的而進行聆訊，而

訊應公開進行[339]：

(1) 專員考量個案中的所有情況，認為調查不應公開。

(2)（如調查是由投訴引發的）投訴人以書面要求調查不得公開。

7、強制處分權—傳喚證人

專員為調查之目的，得傳喚其認為能就該目的提供資訊之人，如該調查係經投訴所引發者，得傳喚投訴人及／或其代理人，並對受傳喚之證人進行訊問或規定其向專員提交任何資訊，或向專員出示專員認為與調查目的相關且係由該受傳喚之證人掌管或控制之文件及物品[340]。但如該調查係經投訴所引發，且所涉及之個人資料的全部或一部為條例第 61 條第（1）款所稱為新聞活動目的而由資料使用者持有之個人資料，並得豁免受條例規範時，受傳喚之證人在符合特定條件下得不向專員提供資料或出示文件及物品[341]。

為調查目的而提供資訊、回答問題及出示文件或物品之人，原則上享有香港高等法院民事法律程序中的證人權利[342]。且除就某人經宣誓（類似我國之具結）作出的證詞而對該人控以偽證罪的刑事程序，或對該人控以違反條例刑責的刑事程序外，該人或其他任何人在調查

沒有任何人有向專員發言的當然權利」。

339 香港，個人資料(私隱)條例，第 43 條第(2)款。

340 香港，個人資料(私隱)條例，第 44 條第(1)款。

341 香港，個人資料(私隱)條例，第 44 條第(2)款。

342 香港，個人資料(私隱)條例，第 45 條第(1)款。

過程中作出之陳述或給予之答案，均不得在任何香港裁判官前或在任何法庭、研訊或法律程序中採為對該人之證據[343]。

又專員可支付投訴人及／或其代理人與證人在調查過程中所產生的合理支出[344]。

8、告知視察或調查結果

專員在完成視察或調查後，應以適當方式在合適時間內將下列事項告知資料使用者[345]：

(1) 該視察或調查之結果。

(2) 專員認為適合作出關於促進資料使用者遵守條例規範之任何建議。

(3) 專員擬依據條例第 48 條發表的任何報告。

(4) 專員認為適合的任何其他評論。

(5) 如在調查的狀況，專員是否已決定因應該調查而向資料使用者送達執行通知（見下述），或於告知調查結果時一併送達執行通知[346]。

如專員完成一項由投訴引發之調查，且投訴人未撤回其投訴時[347]，專員應以適當方式在合適時間內將下列

[343] 香港，個人資料(私隱)條例，第 45 條第(2)款。
[344] 香港，個人資料(私隱)條例，第 44 條第(9)款。
[345] 香港，個人資料(私隱)條例，第 47 條第(1)款、第(2)款。
[346] 香港，個人資料(私隱)條例，第 47 條第(2A)款。
[347] 香港，個人資料(私隱)條例，第 47 條第(3A)款。

事項告知投訴人[348]：

(1) 該調查之結果。

(2) 專員向資料使用者作出之建議。

(3) 專員擬依據條例第 48 條發表的任何報告。

(4) 資料使用者對該等建議或報告之任何評論。

(5) 專員有無或是否已決定因應該調查而對資料使用者送達執行通知。

(6) 如專員未對資料使用者送達執行通知，且已決定不送達執行通知，則投訴人可向香港行政上訴委員會提出上訴以反對之權利[349]。

(7) 專員認為適合的任何其他評論。

但若專員對資料使用者之行為完成調查後，發現其行為因條例第 8 部規定而得豁免適用條例規範，且如依前述規定將各事項告知資料使用者或投訴人將有相當可能損害該豁免所保障之利益時，專員應以適當之方式於合適之時間向資料使用者告知該調查結果及其他評論，並向投訴人（如有）告知專員調查之結果係該資料使用者之行為不屬違反條例之規定[350]。

9、視察及調查報告

---

348 香港，個人資料(私隱)條例，第 47 條第(3)款。
349 香港，個人資料(私隱)條例，第 47 條第(4)款。
350 香港，個人資料(私隱)條例，第 49 條。

專員就屬於某資料使用者類別之資料使用者使用的個人資料系統完成視察後，得以合適之方式發表記載專員認為可促進該類別資料使用者遵守條例規定之任何建議的報告[351]。

又專員在對資料使用者之行為完成調查後，如認符合公共利益時，得以合適之方式發表記載調查結果、專員認為可促進某類別資料使用者遵守條例規定之任何建議及專員認為適合的任何其他評論之報告[352]。

前述報告須以避免能由報告中確定任何個人身分（不含專員或其僱用之人或資料使用者）之方式呈現[353]。

但若專員對資料使用者之行為完成調查後，發現其行為因條例第 8 部規定而得豁免適用條例規範，且如依前述規定發表報告將有相當可能損害該豁免所保障之利益時，專員即無須發表報告[354]。

10、執行通知

專員對資料使用者之行為完成調查後，如認其已違反或正在違反條例規定時，得在考量該違反情形是否已對或有相當可能對資料當事人造成損害或困擾後[355]，決定是否向資料使用者送達書面執行通知並記載

[351] 香港，個人資料(私隱)條例，第 48 條第(1)款。
[352] 香港，個人資料(私隱)條例，第 48 條第(2)款。
[353] 香港，個人資料(私隱)條例，第 48 條第(3)款、第(4)款。
[354] 香港，個人資料(私隱)條例，第 49 條。
[355] 香港，個人資料(私隱)條例，第 50 條第(2)款。

下列事項[356]，以命其改正及（如適當）防止再發生違反情形[357]，亦可以書面通知撤銷該執行通知[358]：

(1) 專員認為違反條例之意見及理由。

(2) 專員認為正在或已遭違反之規定及構成該違反的作為或不作為。

(3) 資料使用者應採取何步驟以改正該違反情形，及（如適當）如何防止該違反情形再發生。前述步驟可藉提出任何經核准的實務守則而擬訂，亦可按所需形式擬訂，以讓資料使用者從不同方式中選擇[359]。

(4) 須在何日或之前採取前述步驟。但該日期不得早於執行通知送達資料使用者後 14 天內，即資料使用者得向行政上訴委員會提出上訴反對該通知之期間[360]，且如資料使用者在期限內提出上訴時，在該上訴決定或撤回前不需採取前述步驟[361]。惟如專員認有特殊情況，因事態緊急而須立即採取前述步驟時（即不受前述送達後 14 天期限之拘束），應在執行通知中加入該立即採取步驟之陳述及理由，但不得規定資料使用者須在送達當日起算 7 日期間內

356 香港，個人資料(私隱)條例，第 50 條第(1A)款。
357 香港，個人資料(私隱)條例，第 50 條第(1)款。
358 香港，個人資料(私隱)條例，第 50 條第(6)款。
359 香港，個人資料(私隱)條例，第 50 條第(3)款。
360 香港，個人資料(私隱)條例，第 50 條第(1B)款、第(7)款。
361 香港，個人資料(私隱)條例，第 50 條第(4)款。

採取該步驟[362]。

(5) 本條（條例第 50 條執行通知）之規定。

又如專員在調查完成前認為資料使用者正在或已經違反條例規定，且因有特殊情況而事態緊急，應立即將執行通知送達資料使用者時，即便調查未完成，專員亦可向資料使用者送達執行通知，但須在不損害須加入該通知的其他事項的原則下，於通知中載明專員認事態緊急應立即發出執行通知之理由[363]。

11、處罰

(1) 違反執行通知

資料使用者若違反執行通知即構成犯罪行為，經首次定罪可處第 5 級罰款及監禁 2 年，如犯罪行為在定罪後仍持續，可每日處罰款 1000 元；若經再次定罪，可處第 6 級罰款及監禁 2 年，如犯罪行為在定罪後仍持續，可每日處罰款 2000 元[364]。但遭控之資料使用者如能證明自己已作出一切努力以遵從執行通知者，即可免責[365]。

又資料使用者在遵從某執行通知後，故意作出某作為或有某不作為，違反條例之規定，且該作為或不作為係執行通知中之記載相同時，亦屬犯罪行

362 香港，個人資料(私隱)條例，第 50 條第(5)款。
363 香港，個人資料(私隱)條例，第 50 條第(8)款。
364 香港，個人資料(私隱)條例，第 50A 條第(1)款。
365 香港，個人資料(私隱)條例，第 50A 條第(2)款。

為，一經定罪可處第 5 級罰款及 2 年監禁，如犯罪行為在定罪後仍持續，可每日處罰款 1000 元[366]。

(2) 其他刑事責任

任何人如有下列情況即構成犯罪行為，一經定罪可處第 3 級罰款及監禁 6 個月[367]：

A. 該人無合法辯解而妨礙、阻撓或抗拒專員或專員僱用之人執行視察、調查之任務或行使權力。

B. 該人無合法辯解而未遵從專員或專員僱用之人為視察或調查所作的合法要求。

C. 該人在專員或專員僱用之人執行視察、調查之任務或行使權力的過程中作出虛假陳述或以其他方式在知情下誤導專員或專員僱用之人。

(三) 實務研究

專員須為精進其任務而研究及監察資料處理與資訊科技的發展，以審酌該發展對個人隱私保護可能產生的不利影響[368]。

366 香港，個人資料(私隱)條例，第 50A 條第(3)款。
367 香港，個人資料(私隱)條例，第 50B 條。
368 香港，個人資料(私隱)條例，第 8 條第(1)(f)款。

第五節　澳門—個人資料保護辦公室

一、概述

澳門於 2007 年由行政長官以第 83/2007 號行政長官批示設立個人資料保護辦公室（以下簡稱個資辦），存續期間為三年，但可續期[369]，在澳門行政長官監督下獨立運作，負責行使 2005 年生效之澳門《個人資料保護法》（以下簡稱個資法）的法定職權，並監察、協調對個資法的遵守及執行[370]。

二、監管對象與主管法規

個資辦依個人資料保護法規定，監管公務機關與非公務關，並得依法予以處罰；又除個人資料保護法外，未監管其他澳門法律。

三、組織規範

(一) 地位與首長

依批示規定，個資辦為澳門公共行政架構中的「項目組」性質[371]，即由公務員及專為執行個資法事項而以合約方式聘用之人員組成（任務編組）。

個資辦在行政長官監督下獨立運作[372]，並由行政長官批示定期委任的一名主任領導及一名副主任輔助[373]，正、副主

---

369 澳門，第 83/2007 號行政長官批示，第 1 條。
370 澳門，第 83/2007 號行政長官批示，第 2 條。
371 澳門，第 83/2007 號行政長官批示，第 1 條。
372 澳門，第 83/2007 號行政長官批示，第 3 條。
373 澳門，第 83/2007 號行政長官批示，第 4 條。

任的職務得為兼任[374]。

正、副主任之報酬由行政長官訂定[375]，個資辦主任於2017年之每月薪俸點與澳門第15/2009號法律《領導及主管人員通則的基本規定》中的局長薪俸點相同為1100點[376]，依新聞所載2017年之換算基準，薪俸點每點為澳門幣83元[377]，計澳門幣91,300元，約新台幣34萬元。

(二) 人員任用

個資辦的人員係由主任建議，經由下列方式任用[378]：

1、向所屬部門徵用或派駐。

2、依《澳門公共行政工作人員通則》規定訂定行政任用合同。

3、包工合同或個人勞動合同。

(三) 預算

個資辦之設置及運作所需經費由澳門特別行政區預算登錄之撥款支付，必要時由財政局調動撥款[379]。個資辦應每年向監督機關提出工作所需的預算提案以便納入澳門特別行政區預算內[380]。

---

374 澳門，第83/2007號行政長官批示，第5條。
375 澳門，第83/2007號行政長官批示，第6條。
376 澳門，第209/2017號行政長官批示，第2條。
377 見 https://thestandnews.com /澳門/澳門明年政府續派九千元公務員獲加薪 2-5/，最後到訪日為106年8月14日。
378 澳門，第83/2007號行政長官批示，第7條。
379 澳門，第83/2007號行政長官批示，第8條。
380 澳門，第83/2007號行政長官批示，第9條。

四、法定職務

(一) 作出許可

依澳門個資法規定，個資辦應就下列事項決定是否作出許可：

1、許可負責處理資料之實體[381]為歷史、統計或科學之目的，基於正當利益而要求延長個人資料的保存期限[382]。

2、許可負責處理資料之實體基於重大公共利益且為行使其職責及權限所必須而處理敏感性個資[383]。

3、考量負責處理資料之實體是否能夠確保足以保障他人私人生活、基本權利和自由之機制（尤指經由契約方式確保權利行使），以決定是否許可負責處理資料之實體將個人資料傳輸至澳門以外、無法確保具備適當保護程度之法律體系的第三方[384]。

4、除法律規定或具組織性質的規章規定之外，關於資料當事人信用和償付能力資料的處理應經個資辦許可[385]。

5、將一個資料庫的資料與其他一個或多個負責實體的一個或多個資料庫的資料聯繫、或與同一負責實體但目的不同之資料庫的資料聯繫而處理資料時，應經個資辦許

---

381 指「就個人資料處理的目的和方法，單獨或與他人共同做出決定的自然人或法人，公共實體、部門或其他任何機構」，類同我國個人資料保護法定義之蒐集機關。參澳門個人資料保護法，第 4 條第 1 款第 5 項。

382 澳門，個人資料保護法，第 5 條第 2 款。

383 澳門，個人資料保護法，第 7 條第 2 款第 2 項。

384 澳門，個人資料保護法，第 20 條第 2 款。

385 澳門，個人資料保護法，第 22 條第 1 款第 2 項。

可[386]。

6、負責處理資料之實體在與蒐集資料之目的不同的情況下使用個人資料，應經個資辦許可[387]。

(二) 接受通知

依澳門個資法規定，個資辦應接受負責處理個人資料之實體就下列事項所為之通知：

1、基於統計、歷史或科學研究之目的而處理個資時，在不可能告知資料當事人或作出告知的成本過高，又或當法律或行政法規明確規定資料的登記或公開時，雖得免除澳門個資法規定告知法定事項之義務，但須對個資辦作出通知[388]。

2、符合澳門個資法第 20 條第 1 款所訂要件而得例外將個人資料傳輸至澳門以外、無法確保具備適當保護程度之法律體系的第三方時，須對個資辦作出通知[389]。

3、為實現一個或數個相關聯之目的而進行的一個或一系列、全部或部分自動化處理個人資料，應於開始處理個資起 8 日內，對個資辦作出通知[390]。

4、為保護資料當事人或其他人重大利益所須，且資料當事人在身體上或法律上無能力作出同意時，例外得處理資

386 澳門，個人資料保護法，第 22 條第 1 款第 3 項。
387 澳門，個人資料保護法，第 22 條第 1 款第 4 項。
388 澳門，個人資料保護法，第 10 條第 5 款第 3 項。
389 澳門，個人資料保護法，第 20 條第 1 款。
390 澳門，個人資料保護法，第 21 條第 1 款。

料當事人的敏感性個資，但須對個資辦作出通知[391]。

(三) 決定跨境傳輸個資地區

依澳門個資法第 19 條規定，負責處理資料之實體僅得在接受資料方當地的法律體系能確保適當的保護程度下，始能將個人資料傳輸至澳門以外之第三方。而某法律體系是否能確保適當保護程度即由個資辦決定[392]。

(四) 提出意見書

依澳門個資法規定，負責處理資料之實體得向個資辦申請請求發出意見書[393]。

(五) 制並／或登記行為守則

依澳門個資法規定,個資辦鼓勵及支持制定行為守則，以便依各業別特性執行個資法規定，同時個資辦亦接受、審查專業團體和其他組織送交之行為守則以作出登記，但經登記之行為守則並不具有法律規範或規章規範之性質[394]。

(六) 提出年度報告

依澳門個資法規定，個資辦應在其年度報告中公布所有依個資法規定編制的意見書和發出的許可[395]。

---

391 澳門，個人資料保護法，第 21 條第 5 款。
392 澳門，個人資料保護法，第 19 條第 3 款。
393 澳門，個人資料保護法，第 23 條。
394 澳門，個人資料保護法，第 26 條、第 27 條。
395 澳門，個人資料保護法，第 25 條第 5 款。

(七) 處罰

1、行為人在個資辦為履行個資法或其他保護個人資料法例規定的義務而訂定的期間完結後，仍不履行義務者，即構成刑事責任，最高可處一年徒刑或 120 日罰金[396]。

2、行為人在個資辦通知不得再讓沒有遵守個資法規定者查閱之後，負責處理個人資料的實體繼續讓有關人士查閱其傳送資料的公開網絡，即構成刑事責任，最高可處一年徒刑或 120 日罰金[397]。

3、行為人經通知後無合理理由拒絕對個資辦提出具體要求合作，即構成加重刑事責任[398]。

[396] 澳門，個人資料保護法，第 37 條第 1 款第 5 項。
[397] 澳門，個人資料保護法，第 37 條第 1 款第 6 項。
[398] 澳門，個人資料保護法，第 40 條第 2 款第 1 項。

第六節　日本─個人資訊保護委員會

一、概述

日本於 2015 年 9 月 3 日通過新修正之《個人資訊保護法》（日文：個人情報の保護に関する法律）[399]，並於 2016 年 1 月 1 日設置個人資訊保護委員會（日文：個人情報保護委員会，下稱委員會）為內閣府外局之委員會，由內閣總理大臣（首相）管轄，對全體民間事業進行監督確保其遵守法令及訂立適當自律規範等，並統一法律解釋及適用，基此，委員會立於個資法中央主管機關之地位，原由各事業主務大臣各自訂立的準則（日文：ガイドライン），今後由委員會將之統一定出基本規則，必要時再訂立專門領域之個別準則。如因規範專業領域之法律亦有關於個資處理之問題時，其準則之訂定則由委員會提出意見，與該事業主管機關共管之[400]。

《個人資訊保護法》第 59 條至第 74 條規定委員會之設置、任務、職權、獨立性、組織、任期、身分保障、罷免、委員長、會議、專門委員、事務局、中立性、保密義務、薪俸、訂定規則等事項。

二、監管對象及主管法規

委員會負責《個人資訊保護法》之執行實施，依該法監管日本民間事業，而公務機關則非屬委員會監管對象，日本另訂定《行政機關個人資料保護法》、《獨立行政法人等個人資料保護法》等

---

399 日本將「information」翻譯為「情報」，故本文將日文「情報」均譯為「資訊」。

400 日本原無個資保護專責機關，後制定有關個人番號之「番號法」，先成立特定個人資訊保護委員會，再修訂個人資訊保護法後，改組成為個人資訊保護委員會。

規範公務機關及行政法人,並由總務省行政管理局掌理中央行政機關及獨立行政法人之個人資料保護法律[401]。

三、組織規範

(一) 地位

《個人資訊保護法》第 59 條將委員會定位為依《內閣府設置法》第 49 條第 3 項規定設置之內閣府外局機關，由內閣總理大臣及首相管轄[402]，具有高度獨立性，並具有獨立的法人地位，相當於我國中央二級獨立機關，即中央選舉委員會、公平交易委員會、國家通訊傳播委員會。

又《個人資訊保護法》第 65 條給予委員長及委員身分上保障，此外，因委員會係屬內閣總理大臣轄下之行政委員會，為除去可能受干擾之疑慮，同法第 62 條明定委員會之委員長及委員獨立行使職權[403]。

另因委員會除須排除政治力干預，獨立行使職權外，尚須保持中立性，不得代表任何政治團體或與任何利益團體，始能獲得人民之信賴，故同法第 71 條規定，委員長及

---

401 第２条
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、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 15 年法律第 59 号）第２条１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 15 年法律第 118 号）第２条第１項に規定する地方独立行政法人をいう。以下同じ。）

402 第 59 条内閣府設置法第 49 条第３項の規定に基づいて、個人情報保護委員会を置く。
２委員会は、内閣総理大臣の所轄に属する。

403 第 62 条委員会の委員長及び委員は、独立してその職権を行う。

委員在任期中不得擔任政黨或其他政治團體之幹部，或積極從事政治運動；且委員長及委員在任期中除非獲內閣總理大臣許可，否則不得從事有酬之其他職務、經營營利事業，或執行其他以金錢利益為目的之業務[404]。

(二) 任免

《個人資訊保護法》第 63 條規定，委員會由委員長 1 人及委員 8 人組成，其中 4 人為兼任委員[405]。委員及委員長須經參、眾議院同意後，由首相任命之。同法第 64 條規定，委員及委員長任期為 5 年，且得連任[406]。另同法第 65 條給予委員長及委員身分保障，除有下列情況，否則不得違反本人意願予以免職[407]：

1、受破產程序開始之處分。

---

404 第 71 条委員長及び委員は、在任中、政党その他の政治団体の役員となり、又は積極的に政治運動をしてはならない。
2 委員長及び常勤の委員は、在任中、内閣総理大臣の許可のある場合を除くほか、報酬を得て他の職務に従事し、又は営利事業を営み、その他金銭上の利益を目的とする業務を行ってはならない。

405 第 63 条委員会は、委員長及び委員８人をもって組織する。
2 委員のうち４人は、非常勤とする。
3 委員長及び委員は、人格が高潔で識見の高い者のうちから、両議院の同意を得て、内閣総理大臣が任命する。

406 第 64 条委員長及び委員の任期は、５年とする。ただし、補欠の委員長又は委員の任期は、前任者の残任期間とする。
2 委員長及び委員は、再任されることができる。

407 第 65 条委員長及び委員は、次の各号のいずれかに該当する場合を除いては、在任中、その意に反して罷免されることがない。
一破産手続開始の決定を受けたとき。
二この法律又は番号利用法の規定に違反して刑に処せられたとき。
三禁錮以上の刑に処せられたとき。
四委員会により、心身の故障のため職務を執行することができないと認められたとき、又は職務上の義務違反その他委員長若しくは委員たるに適しない非行があると認められたとき。

2、違反本法或個人編號法而被處以刑罰。

3、受有期徒刑之宣告。

4、被委員會認定身心障礙無法執行職務，或有違反職務上義務及其他不適任行為者。

為免前述第(4)項事由遭到濫用並保障委員會之獨立性，該項事由是否成立，係由之委員會自行判斷，且委員會之決定依《個人資訊保護法》第 68 條第 4 項規定，必須經本人以外之其他委員全體同意。

(三) 薪俸

《個人資訊保護法》第 73 條規定，委員長及委員之薪俸另由法律定之，委員長的每月薪俸 1,199,000 日元，與日本大臣政務官（相當於我國）同等，專任委員的每月薪俸 1,035,000 日元[408]。

(四) 成員

《個人資訊保護法》第 70 條規定，委員會設置事務局以協助委員調查或處理行政事務[409]。2016 年初委員會成立時，事務局設置 52 位人員，同年底增加至 78 位，2017 年末增加至 103 位[410]，2018 年末則預計增加至 119 位[411]。事

---

408 《特別職の職員の給与に関する法律》別表第一（第三条関係）。

409 第 70 条委員会の事務を処理させるため、委員会に事務局を置く。
2 事務局に、事務局長その他の職員を置く。
3 事務局長は、委員長の命を受けて、局務を掌理する。

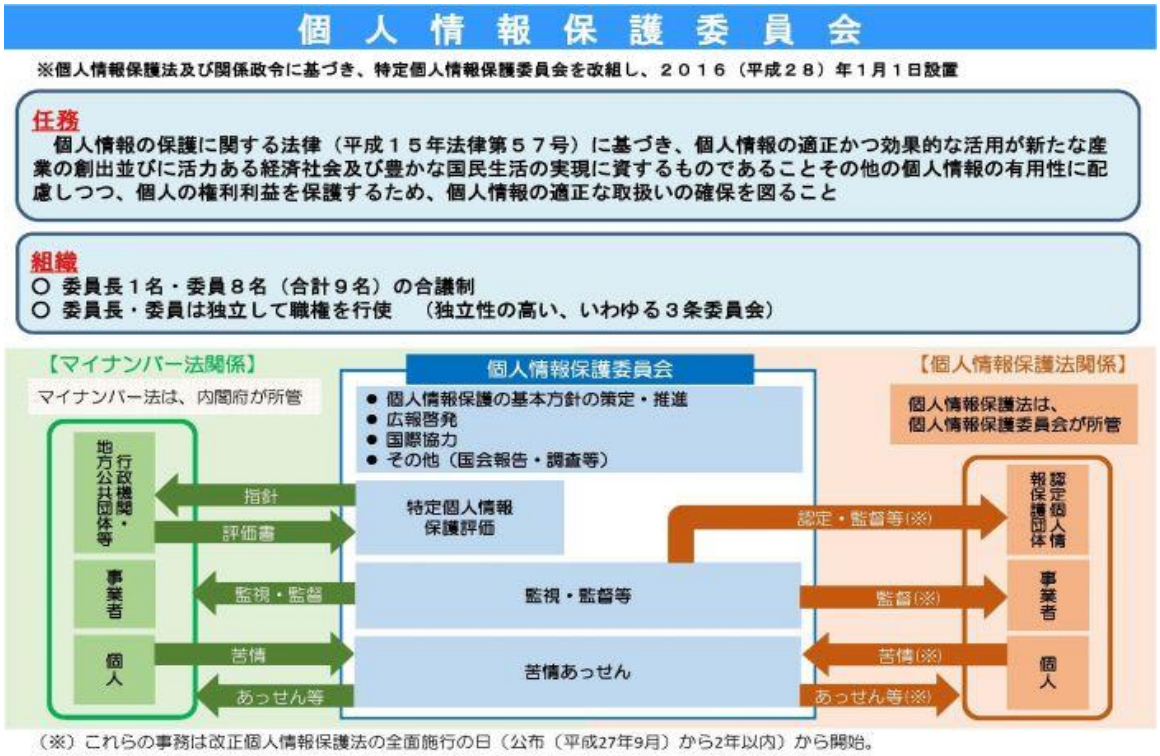
410 平成 29 年度予算案・機構定員の概要，網址：https://www.ppc.go.jp/files/pdf/161222yosan-kikouteiin.pdf，最後到訪日為 106 年 7 月 25 日。

411 平成 30 年度予算案・機構定員の概要，網址：

務局目前設有事務局長１人，次長１人，總務課長１人，以及參事官３人。另同法第 69 條規定，委員會得針對專門事項之調查設置兼任專門委員，由委員會提出申請後經內閣總理大臣任命，惟其於專門事項調查結束後即解任[412]。目前委員會設有三位兼任專門委員負責國際合作事宜。

圖 3 日本個人資訊保護委員會組織說明圖

四、法定職務



委員會所掌事務按《個人資訊保護法》第 61 條規定如下[413]：

---

https://www.ppc.go.jp/files/pdf/171222yosan-kikouteiin.pdf，最後到訪日為 107 年 1 月 15 日。

412 第 69 条委員会に、専門の事項を調査させるため、専門委員を置くことができる。
２専門委員は、委員会の申出に基づいて内閣総理大臣が任命する。
３専門委員は、当該専門の事項に関する調査が終了したときは、解任されるものとする。
４専門委員は、非常勤とする。

413 第 61 条委員会は、前条の任務を達成するため、次に掲げる事務をつかさどる。

(一) 基本方針之制定及推展。

(二) 有關個資及匿名加工資料處理之監督，及對當事人提出申訴進行必要之斡旋，並協助業者處理。

(三) 有關個資保護團體之認定、監督事宜。

(四) 特定個資處理之監視、監督，或對當事人提出申訴進行必要之斡旋，並協助業者處理。

(五) 特定個資保護評價。

(六) 對個資之保護及適當、有效率之活用，進行宣導。

(七) 對有關實施前六項事務，進行必要之調查及研究。

(八) 有關所掌職務之國際協助事項。

一基本方針の策定及び推進に関すること。
二個人情報取扱事業者における個人情報の取扱い並びに個人情報取扱事業者及び匿名加工情報取扱事業者における匿名加工情報の取扱いに関する監督、行政機関の保有する個人情報の保護に関する法律第２条第１項に規定する行政機関における同条第９項に規定する行政機関非識別加工情報(同条第 10 項に規定する行政機関非識別加工情報ファイルを構成するものに限る。）の取扱いに関する監視、独立行政法人等における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第２条第９項に規定する独立行政法人等非識別加工情報（同条第 10 項
に規定する独立行政法人等非識別加工情報ファイルを構成するものに限る。）の取扱いに関する監督並びに個人情報及び匿名加工情報の取扱いに関する苦情の申出についての必要なあっせん及びその処理を行う事業者への協力に関すること（第４号に掲げるものを除く。)。
三認定個人情報保護団体に関すること。
四特定個人情報(番号利用法第２条第８項に規定する特定個人情報をいう。第 63 条第４項において同じ。）の取扱いに関する監視又は監督並びに苦情の申出についての必要なあっせん及びその処理を行う事業者への協力に関すること。
五特定個人情報保護評価(番号利用法第 27 条第１項に規定する特定個人情報保護評価をいう。）に関すること。
六個人情報の保護及び適正かつ効果的な活用についての広報及び啓発に関すること。
七前各号に掲げる事務を行うために必要な調査及び研究に関すること。
八所掌事務に係る国際協力に関すること。
九前各号に掲げるもののほか、法律（法律に基づく命令を含む。）に基づき委員会に属させられた事務。

(九) 除前揭事項外之其他依法屬於委員會之事務。

(十) 監督權限

1、要求業者提出報告及實地查核：

按《個人資訊保護法》第 40 條第 1 項規定，委員會對個資處理業者或匿名加工資料處理業者，關於《個人資訊保護法》所規定義務之履行等事宜，有應予改善而進行檢討之問題時，得於必要範圍要求該等業者提出報告或相關資料，或實地至其營業處所或其他必要之處所詢問其職員，或查核帳冊、書類及其他物件（如電腦設施）等[414]。

前述實地查核僅限於委員會要求業者提出報告後仍無法掌握正確事實，或蒐集必要資料仍有困難時方得實施。若業者拒絕提出報告或拒絕受檢，依同法 85 條規定得處 30 萬日圓以下罰金。另依同法第 40 條第 3 項規定，前述檢查行為並非調查犯罪調查，故無須得到法院許可，但其檢查所得之資料，並不完全排除於將來訴訟時作為證明犯罪之用[415]。

2、指導及建議

---

414 第 40 条個人情報保護委員会は、前二節及びこの節の規定の施行に必要な限度において、個人情報取扱事業者又は匿名加工情報取扱事業者（以下「個人情報取扱事業者等」という。）に対し、個人情報又は匿名加工情報（以下「個人情報等」という。）の取扱いに関し、必要な報告若しくは資料の提出を求め、又はその職員に、当該個人情報取扱事業者等の事務所その他必要な場所に立ち入らせ、個人情報等の取扱いに関し質問させ、若しくは帳簿書類その他の物件を検査させることができる。

415 第 40 条
3 第1項の規定による立入検査の権限は、犯罪捜査のために認められたものと解釈してはならない。

按《個人資訊保護法》第 41 條規定，委員會得對個資處理業者或匿名加工資料處理業者，提出有關個資匿名加工資料處理方面必要之指導及建議[416]。此指導及建議並非行政處分，亦無法律拘束力，目的係希望業者可自主改善不當處理個資之行為。

3、勸告及命令

《個人資訊保護法》第 42 條規定個資處理業者或匿名加工資料處理業者違反相關規定時，委員會為確保正當處理個資或匿名加工資料而認為有必要時，得勸告該等業者採取改正或中止違法行為之必要措施。接受勸告者無正當理由而未採取勸告措施，且被認為對個人重大權益有迫切之侵害時，得命令其採取有關勸告之措施，原則上命令採勸告前置主義。但如個資處理業者或匿名加工資料處理業者違反第 16 條、17 條、第 20 條至 22 條、第 23 條第 2 項、第 24 條，或 36 條第 1 項、第 2 項、或第 5 項、第 38 條，且被認為對個人重大權益有危害之事實，有必要採取緊急措施時，委員會得直接命令對該等業者採取中止或改正違法行為之必要措施。對違反本條命令之行為人，得依同法第 84 條規定處以 6 個月以下之拘役，或 30 萬日圓以下罰金。

另原由各事業領域主務大臣制定之準則[417]，則改由委員會依

[416] 第 41 条個人情報保護委員会は、前二節の規定の施行に必要な限度において、個人情報取扱事業者等に対し、個人情報等の取扱いに関し必要な指導及び助言をすることができる。
[417] ガイドライン。

照《個人資訊保護法》第 74 條制定業界通用之準則，如遇有特殊之事業領域則再由該事業主務大臣協助共同訂定[418]。

綜上所述，委員會於必要時，得對處理個人資料之業者採取提供指導及建議、要求其提交報告、提出勸告、進行實地查核或發布命令等漸進式之監管措施，如委員會認為業者違反個人資訊保護法相關規定而不遵從其勸告，或對個人權益有重大影響時，得命令其採取中止或改正違法行為之必要措施，違者得處以 6 個月以下之拘役，或 30 萬日圓以下罰金；另委員會對業者提出詢問或要求其提交報告時，如有虛假、隱匿或不回應，或拒絕、阻礙、迴避委員會進行現場調查等情事，亦得處 30 萬日圓以下罰金。

[418] 第 74 条委員会は、その所掌事務について、法律若しくは政令を実施するため、又は法律若しくは政令の特別の委任に基づいて、個人情報保護委員会規則を制定することができる。

第七節　南韓—個人資訊保護委員會（PIPC）

一、概述

南韓個人資訊保護委員會（Personal Information Protection Committee，PIPC）為南韓個資保護專責機構，其隸屬於總統辦公室，直接對總統負責，位階超乎一般部會，以期有效發揮功能，充分監督個人資料保護相關事務之推動工作。其主要工作包括擬訂個人資料保護政策、就相關法規之實施及修正進行評估、監測違反資料保護法規之行為並調解處理相關損害，及確保資料保護法規之妥善解釋及執行，以保障人民個資安全。此外，個人資訊保護委員會亦就個資保護議題促進國際交流合作。

個人資訊保護委員會係依據《個人資訊保護法（Personal Information Protection Act）》第 7 條第 1 項規定設置[419]，以審議並解決有關個人資料保護之各項事宜。

二、監管對象與主管法規

南韓個人資訊保護委員會僅職司《個人資訊保護法》之監管，且僅監督南韓政府各公務機關主管之法規，是否可能影響國民之個資保護，並無裁罰之能力。

三、組織規範

(一) 地位

[419] Republic of Korea, Personal Information Protection Act, Article 7(1), "The Personal Information Protection Commission (hereinafter referred to as the ‘Commission’) shall be established under the Presidential Office to deliberate and resolve the matters regarding data protection. The Commission shall independently conduct the functions belonging to its authority".

依據南韓《個人資訊保護法》第 7 條第 1 項規定[420]，個人資訊保護委員會隸屬於總統辦公室，獨立行使職權，其地位近似於我國總統府國家安全會議。

(二) 任免

依據南韓《個人資訊保護法》第 7 條第 2 項規定[421]，個人資訊保護委員會由 15 名以下之委員組成，其中包含一名主席及一名常任委員；後者係政治任命官員，前者則依據第 7 條第 3 項規定[422]，由總統自非政治任命之委員中委派。

此外，同法第 7 條第 4 項規定[423]，個人資訊保護委員人選可由與隱私相關之公民團體及消費者團體，或個人資料處理業者之產業公會或協會推薦，或由其他具豐富之資料保護學術知識及經驗人士出任；委員之指派係屬總統職權，但總統必須由國會篩選出之人選中指派 5 位委員，另自最高法院首席大法官指定之人選中亦指派 5 位委員。主席及委員之任期，依第 7 條第 5 項規定為 3 年[424]，可續任一次。

---

420 同前註。

421 Republic of Korea, Personal Information Protection Act, Article 7(2), “The Commission shall consist of not more than 15 Commissioners, including one Chairperson and one Standing Commissioner, who shall be a public official in political service.”

422 Republic of Korea, Personal Information Protection Act, Article 7(3), "The Chairperson shall be commissioned by the President from among non-public official Commissioners."

423 Republic of Korea, Personal Information Protection Act, Article 7(4), "The Commissioners shall be appointed or commissioned by the President from among the persons stated in any of the following Subparagraphs. In this case, five Commissioners shall be appointed or commissioned from among the candidates elected by the National Assembly, and other five Commissioners from among the candidates designated by the Chief Justice of the Supreme Court: 1. Persons recommended by privacy-related civic organizations or consumer groups; 2. Persons recommended by the trade associations composed of personal information processors; and 3. Other persons who have ample academic knowledge and experiences related with personal information."

424 Republic of Korea, Personal Information Protection Act, Article 7(5), "The term of office for the

(三) 組織架構

依據南韓《個人資訊保護法》第 7 條第 6 項規定[425]，個人資訊保護委員會應於主席認為必要時，或超過四分之一委員共同要求時召開會議，會議決議依據第 7 條第 7 項規定[426]，於超過半數以上委員出席時，即由出席委員以多數決；第 7 條第 8 項規定[427]個人資訊保護委員會下設秘書處，以支援其行政運作。

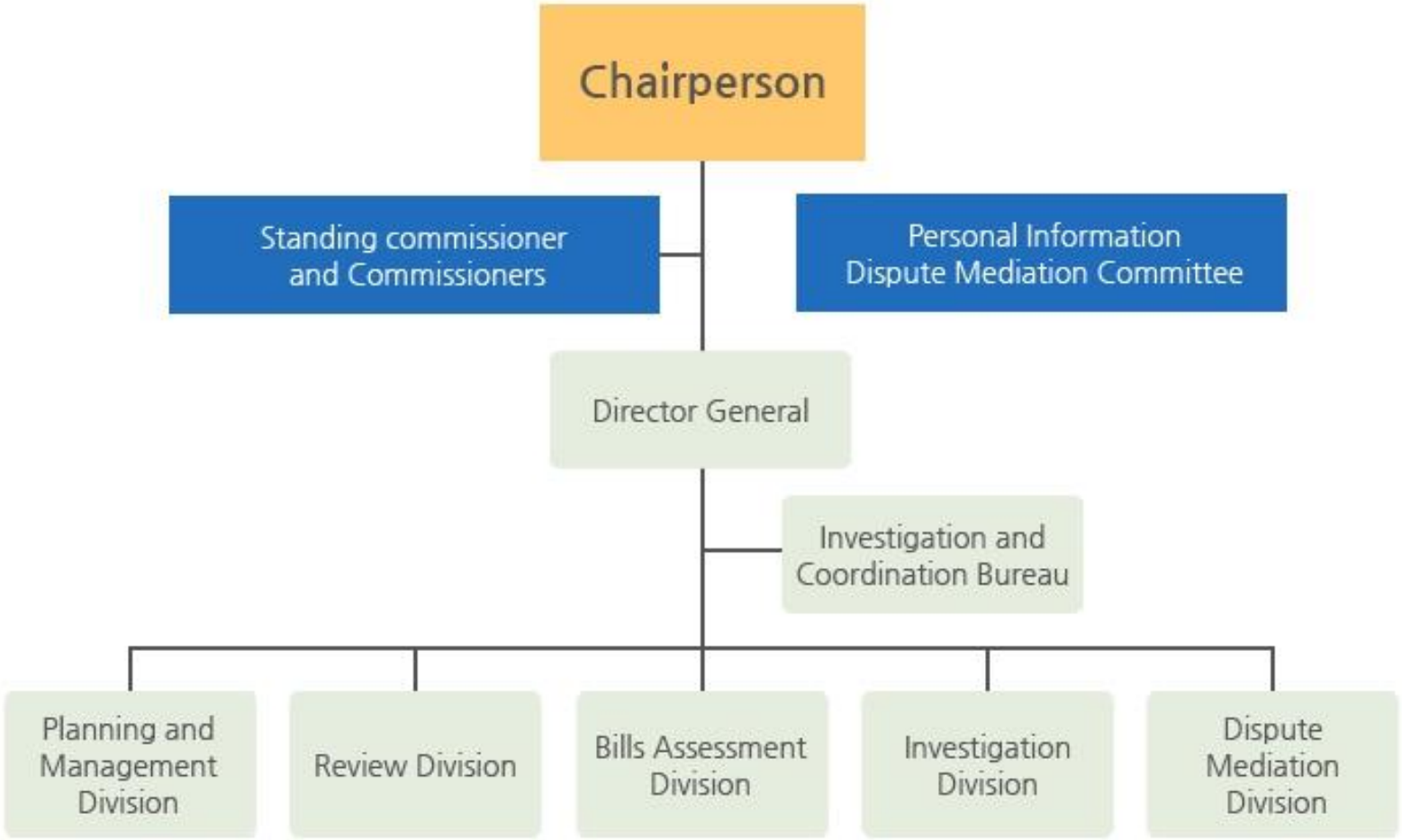
Chairperson and Commissioners shall be three years, and their term of office may be only once extended."

[425] Republic of Korea, Personal Information Protection Act, Article 7(6), "The meeting of the Commission shall be convened by the Chairperson when the Chairperson deems it necessary or more than one quarter of Commissioners demand it."

[426] Republic of Korea, Personal Information Protection Act, Article 7(7), "The resolution of the meeting of the Commission shall be made by the affirmative votes of the majority of present Commissioners if more than half of the Commissioners are present at the meeting."

[427] Republic of Korea, Personal Information Protection Act, Article 7(8), "A secretariat shall be established within the Commission to support the administration of the Commission."

圖 4 南韓個人資料保護委員會組織架構圖



四、法定職務

(一) 依據南韓《個人資訊保護法》第 8 條第 1 項規定[428]，個人資訊保護委員會之功能如下：

1、 依同法第8條之2規定[429]，針對因該法規定生效或修正，造成各部會處理個人資料之政策或體制改變而發生之資安事故，分析評估其發生原因；個人資訊保護委員會依同條規定，亦得就該法或其轄下相關法規之進一步改善事宜，向相關部會首長提出建議；

2、 依同法第 9 條規定[430]，每 3 年與相關部會商議後提出「資

---

[428] Republic of Korea, Personal Information Protection Act, Article 8(1), " The Commission shall deliberate and resolve the following matters: 1. Matters regarding the assessment of data breach incident factors under Article 8-2; 1-2. The Basic Plan under Article 9 and the Implementation Plan under Article 10; 2. Matters for the improvement of policies, systems and legislation related with data protection; 3. Matters for the coordination of positions taken by public institutions with respect to the processing of personal information; 4. Matters regarding the interpretation and operation of laws and regulations related with data protection; 5. Matters regarding the use and provision of personal information under Article 18(2)v; 6. Matters regarding the result of the Privacy Impact Assessment under Article 33(3); 7. Matters regarding the suggestion of opinion under Article 61(1); 8. Matters regarding the advice of measures under Article 64(4); 9. Matters regarding the disclosure of results under Article 66; 10. Matters regarding the making and submission of the Annual Report under Article 67(1); 11. Matters referred to the meeting by the President, the Chairperson of the Commission or more than two Commissioners with respect to data protection; and 12. Other matters to be deliberated and resolved by the Commission under this Act or other laws and regulations."

[429] Republic of Korea, Personal Information Protection Act, Article 8-2, "(1) The head of central administrative departments shall request the Commission to assess the data breach incident factors in case where the policy or system in need of personal information processing is adopted or changed by the enactment or amendment of the Act or subordinate statutes under its jurisdiction. (2) When receiving the request pursuant to paragraph (1), the Commission may, upon the analysis and review of the data breach incident factors of the Act or subordinate statutes concerned, recommend the necessary matters for the improvement of such Act or subordinate statutes to the head of relevant departments concerned. (3) Necessary matters concerning the procedure and method to assess the data breach incident factors pursuant to paragraph (1) shall be provided by the Presidential Decree."

[430] Republic of Korea, Personal Information Protection Act, Article 9, "The Commission shall establish the Data Protection Basic Plan (hereinafter referred to as the "Basic Plan") every three years in consultation with the head of central administrative department or agency concerned to ensure the protection of personal information and the rights and interest of data subjects. (2) The Basic Plan shall include the followings: 1. The basic goals and intended directions of data protection; 2. The improvement of data protection systems and legislation; 3. Countermeasures to prevent privacy

料保護基本計畫」，並審議同法第 10 條規定[431]各部會每年依基本計畫提出之「執行計畫」；個人資訊保護委員會於撰擬前述基本計畫時，另得依同法第 11 條第 1 項規定[432]，針對個資持有者之法規遵循及個資管理情形，要求該等業者、中央政府相關部會首長、地方政府及相關公協會等單位提供資料或建議。

3、改善資料保護政策、體制及立法；且個人資訊保護委員會依據同法第 8 條第 4 項規定[433]，亦得對相關部會提出改善建議，並依同條第 5 項規定[434]，稽查各部會是否確實實施建議之改善措施；

4、協調各公務機關有關個資處理之立場；

5、審議資料保護相關法規之解釋及運作；

---

violation; 4. How to facilitate self-regulation for data protection; 5. How to activate education and public relations for data protection; 6. Training and fostering specialists in data protection; and 7. Other matters necessary for data protection. (3) The National Assembly, the Court, the Constitutional Court and the National Election Commission may establish and implement its own basic plan for data protection of relevant institutions including affiliated entities."

431 Republic of Korea, Personal Information Protection Act, Article 10, "(1) The head of central administrative department or agency shall establish the implementation plan for data protection each year in accordance with the Basic Plan and submit it to the Commission, and shall carry out the implementation plan subject to the deliberation and resolution of the Commission. (2) The matters necessary for the establishment and carrying out of the implementation plan shall be stated by the Presidential Decree."

432 Republic of Korea, Personal Information Protection Act, Article 11(1), "The Commission may, for the efficient establishment of the Basic Plan, request materials or suggestions regarding the actual state of regulatory compliance and personal information management, etc. by personal information controllers from personal information controllers, the head of central administrative department or agency concerned, the head of local governments and relevant institutions or associations, etc."

433 Republic of Korea, Personal Information Protection Act, Article 8(4), "The Commission may, in case of deliberation and resolution of matters subject to paragraph (1) 2, give an advise on such improvement to the relevant institution."

434 Republic of Korea, Personal Information Protection Act, Article 8(5) "The Commission may inspect whether its advice pursuant to paragraph (4) has been implemented or not.

6、審議第 18 條第 2 項第 5 款規定[435]所稱，公務機關為執行法定職務所必須，將個人資料做目的外利用或提供予第三方之相關事宜；

7、審議第 33 條第 3 項規定[436]所稱，內政部長針對其他部會辦理之隱私衝擊評估結果所提供之意見；

8、審議第 61 條第 1 項規定[437]所稱，內政部長針對其他部會主管法規中包含可能影響資料保護之條文所提供之意見；

9、如中央政府部會、地方政府、國會、法院、憲法法院或國家選舉委員會違反本法，依第 64 條第 4 項規定[438]提出改正建議；

10、審議第 66 條規定[439]所稱，有關各部會針對個資處理相關改善建議、改正命令、懲戒建議及罰金等之公布事

---

435 Republic of Korea, Personal Information Protection Act, Article 18(2)v, "Where it is impossible to carry out the work under its jurisdiction as stated in other laws unless personal information processor uses personal information for other purpose than the intended one, or provides it to a third party, and it is subject to the deliberation and resolution of the Commission;

436 Republic of Korea, Personal Information Protection Act, Article 33(3), "The Minister of Interior may provide its opinion subject to the deliberation and resolution of the Commission upon receiving the PIA result as stated in paragraph (1)."

437 Republic of Korea, Personal Information Protection Act, Article 61(1), "The Minister of Interior may provide its opinion to the authority concerned subject to the deliberation and resolution of the Commission when it is deemed necessary with respect to the laws and regulations which contain provisions likely affecting data protection."

438 Republic of Korea, Personal Information Protection Act, Article 64(4), "The Commission may, when the central administrative department and agency, local government, the National Assembly, the Court, the Constitutional Court or the National Election Commission violates this Act, advise the head of the authority concerned to take the relevant measures applicable to any of the subparagraphs of paragraph (1). In this case, upon receiving the advice, the authority concerned shall respect it."

439 Republic of Korea, Personal Information Protection Act, Article 66, "(1) The Minister of Interior may, subject to the deliberation and resolution of the Commission, disclose the advice for improvement pursuant to Article 61, the corrective order pursuant to Article 64, the accusation or disciplinary advice pursuant to Article 65 and the imposition of fine for negligence pursuant to Article 75 and its result, respectively."

宜；

11、依第 67 條第 1 項規定[440]撰擬資料保護政策及執行情形年報，提報國會；

12、審議、處理總統、個人資訊保護委員會主席或 2 名以上委員交付予個人資訊保護委員會會議之議題；

13、其他依據南韓《個人資訊保護法》及其他法規，應由個人資訊保護委員會審議、處理之議題。

此外，依據《個人資訊保護法》第 8 條第 2 項規定[441]，個人資訊保護委員會為執行以上職務，得徵詢官員、專家、公民團體及相關業者之意見，亦得要求取得相關資料。

(二) 依據南韓《個人資訊保護法》第 5 章以下規定，另成立個資爭端調解委員會（Personal Information Dispute Mediation Committee），其主席依據第 40 條第 4 項規定[442]，亦由個人資訊保護委員會主席委派，個人資訊保護委員會另得依同條第 8 項規定[443]，辦理相關爭端案件歸檔及事實調查之必要事

---

[440] Republic of Korea, Personal Information Protection Act, Article 67(1), "The Commission shall prepare for the report each year, based upon necessary materials furnished by the authorities concerned, in relation to the data protection policy measures and implementation thereof, and submit (including transmission via the information and communications networks) it to the National Assembly before the opening of the plenary session."

[441] Republic of Korea, Personal Information Protection Act, Article 8(2), "The Commission may, if necessary for the deliberation and resolution of matters stated in paragraph (1), take measure of the following subparagraphs: 1. Listening to the opinions of relevant public officials, specialists in data protection, civic organizations and related operators; and 2. Request of relevant materials from the authorities concerned or inquiry of facts."

[442] Republic of Korea, Personal Information Protection Act, Article 40(4), "The Chairman shall be commissioned by the Chairperson of the Commission from among the Committee members except public officials."

[443] Republic of Korea, Personal Information Protection Act, Article 40(8), "The Commission may deal with the affairs necessary for dispute mediation including filing of dispute mediation cases and fact finding, etc."

宜。如發現或懷疑有個資法違法事件發生，個人資訊保護委員會依據該法第 63 條第 4 項規定[444]，得要求內政部長或相關部會首長採取除調閱資料外之其他積極性調查措施。

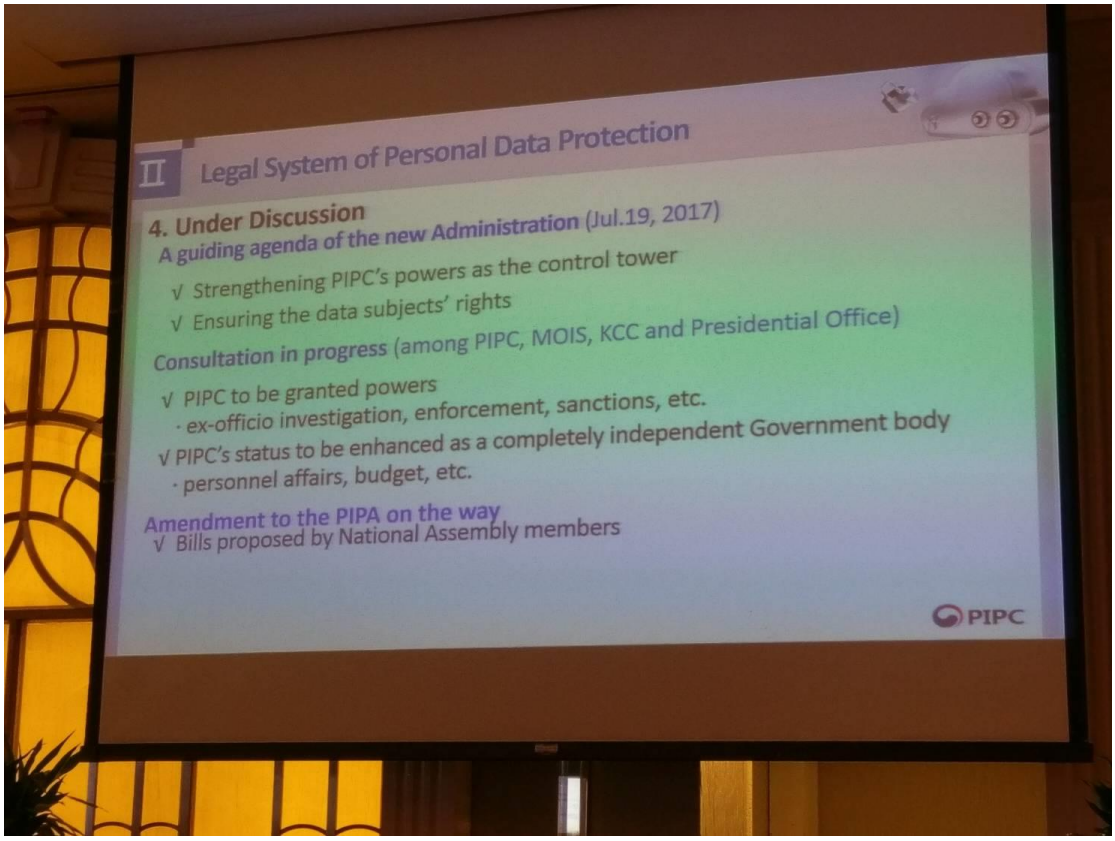
(三) 南韓個資保護委員會係監督南韓政府各公務機關主管之法規，是否可能影響國民之個資保護，並無行政裁罰之能力。另依照南韓個人資料保護法第 75 條第 4 項規定，第 1 至第 3 項之行政罰鍰應依總統命令，由內政部長及一位相關之中央行政機關首長裁定及收取。於此情況下，針對實地個資管控者所處之罰鍰，應由主管之中央行政機關首長裁定及收取[445]。

(四) 不過，本研究團隊成員於 2017 年至香港參加第 39 屆個資與隱私保護委員國際研討會（ICDPPC，詳見本章第十三節）時由南韓個資保護委員會代表簡報內容得知，南韓個資保護委員會刻正尋求相關機關意見，將授予該委員會包含裁罰權在內的更多職權，且更計畫強化其包含人事、預算等面向的獨立地位。

圖 5 南韓個資保護委員會代表於第 39 屆 ICDPPC 簡報

[444] Republic of Korea, Personal Information Protection Act, Article 63(4), “When finding or suspecting any breach of this Act, the Commission may demand the Minister of Interior or the head of central administrative department or agency concerned to take measures pursuant to the part other than each subparagraph of paragraph (1), or paragraph (3). In this case, the Minister of Interior or the head of central administrative department or agency concerned, who was demanded as such, shall respond to it except otherwise exempted by specific circumstances.”

[445] Republic of Korea, Personal Information Protection Act, Ch. IX Article 75 “(4) Administrative fines provided for in paragraphs (1) through (3) shall be imposed and collected by the Minister of the Interior and the head of a related central administrative agency, as prescribed by Presidential Decree. In this case, the head of a related central administrative agency shall impose and collect administrative fines from the personal information controller in the field under his/her jurisdiction” .



五、國際參與

南韓個資保護委員會（PIPC）依據南韓個人資料保護法第 8 條之 2 規定[446]，職權包括監督南韓政府各公務機關主管之法規，是否可能影響國民之個資保護，目前係個資與隱私保護委員國際研討會（ICDPPC，詳見本章第十三節）之會員。韓國網路安全部（Korea Internet and Security Agency，KISA，亦有譯稱網路振

[446] Republic of Korea, Personal Information Protection Act, Art. 8-2, "(1) The head of a central administrative agency shall request the Protection Commission to assess data breach incident factors where the policy or system in need of personal information processing is adopted or changed by the enactment or amendment of any statute under his/her jurisdiction. (2) Upon receipt of a request made pursuant to paragraph (1), the Protection Commission may advise the head of the relevant agency of the matters necessary to improve the relevant statute by analyzing and reviewing the data breach incident factors of such statute. (3) Necessary matters concerning the procedure and method to assess the data breach incident factors under paragraph (1) shall be prescribed by Presidential Decree" .

興院)依據資通訊網路運用及資訊保護等促進法第52條規定[447]，主管資通訊網路之運用及保護事宜,另負責資通訊網路入侵事故因應機制之運作，亦為 ICDPPC 之會員。

韓國廣播通訊委員會（Korea Communications Commission，KCC）依據韓國廣播通訊委員會成立及運作法第 11 條規定[448]，執掌廣播通訊使用者保護、個人資料保護相關倫理等事宜，係 ICDPPC 之觀察員及 APEC 跨境隱私保護執法協議（CPEA，詳見本章第十四節）之成員。韓國內政安全部（Ministry of the Interior and Safety）依據個人資訊保護法第 34-2 條[449]及第 75 條第 4 項規定[450]，針對居民登錄編號等個資事故及違法事項，有權對違反者裁處罰鍰，亦係 ICDPPC 之觀察員及 CPEA 之成員。

---

[447] Republic of Korea, Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., Art. 52, "(3) The Internet and Security Agency shall carry out the following business affairs…5. Information protection for the information and telecommunications network, development of technologies concerning the Internet address resources and standardization thereof;…11. Operation of a system to deal with intrusion cases of information and telecommunications network, analyze the causes thereof, and respond thereto".

[448] Republic of Korea, Act on the Establishment and Operation of Korea Communications Commission, Art. 11, "(1) The following matters shall be duties under the jurisdiction of the Commission: … 2. Matters concerning the overall control of research and planning, market surveys on broadcasting and communications, protection of users of broadcasting and communications, promotion of viewers' rights and interests, and ethics relating to protecting personal information".

[449] Republic of Korea, Personal Information Protection Act, Art. 34-2, "(1) The Minister of the Interior may impose and collect a penalty surcharge not exceeding 500 million won where a personal information controller has caused the loss, theft, divulgence, forgery, alteration, or damage of resident registration numbers: Provided, That this shall not apply where the personal information controller has fully taken measures necessary to ensure safety under Article 24 (3) to prevent any loss, theft, divulgence, forgery, alteration, or damage of such resident registration numbers".

[450] Republic of Korea, Personal Information Protection Act, Art. 75, "(4) Administrative fines provided for in paragraphs (1) through (3) shall be imposed and collected by the Minister of the Interior and the head of a related central administrative agency, as prescribed by Presidential Decree. In this case, the head of a related central administrative agency shall impose and collect administrative fines from the personal information controller in the field under his/her jurisdiction".

第八節　新加坡—個人資料保護委員會（PDPC）

一、概述

新加坡於 2012 年通過《個人資料保護法（Personal Data Protection Act，簡稱 PDPA）》，並於 2013 年 1 月 2 日設立個人資料保護委員會（Personal Data Protection Commission，簡稱 PDPC），此個資保護專責機構之宗旨係為宣導、執行個資保護，以培養企業與消費者間之信任關係，促進新加坡經濟。

依據 2016 年修訂之新加坡《個人資料保護法》第 5 條第 2 項規定[451]，該法之執行由個人資料保護委員會主掌。目前新加坡通訊及新聞部（Ministry of Communications and Information，MCI）下設資通訊媒體發展管理局（Infocommunications Media Development Authority of Singapore, IMDA），新加坡個人資料保護委員會則併入該局管轄。

二、監管對象及主管法規

新加坡《個人資料保護法》僅拘束非公務機關，新加坡個人資料保護委員會僅能對非公務機關施以處罰，但能對新加坡公務機關就個資保護事項提出建議[452]。

此外，由於委員會併入資通訊媒體發展管理局中，因此新加坡《資通訊媒體發展管理法（Infocommunications Media Development Authority Act）》亦由委員會監管。

---

[451] Singapore, Personal Data Protection Act 2012, Section 5(2), "The Personal Data Protection Commission is responsible for the administration of this Act."

[452] Singapore, Personal Data Protection Act, Part II, Section 6, "The functions of the Commission shall be…(c) to advise the Government on all matters relating to data protection".

三、組織規範

(一) 地位

新加坡個人資料保護委員會隸屬於資訊通信媒體發展局（IMDA），而資訊通信媒體發展局（IMDA）隸屬於新加坡通訊及新聞部（MCI），因此新加坡的個人資料保護委員會相當於我國行政院部會下四級行政機關。

另依據新加坡《個人資料保護法》第9條第1項規定[453]，個人資料保護委員會之官員得經檢察官授權後針對違反本法規定之行為採取法律行動；另同條第2項規定，個人資料保護委員會具律師資格之法律顧問，亦得於與個人資料保護委員會行使職權相關之民事訴訟案件中代表個人資料保護委員會[454]。

(二) 人員任免

依據新加坡《個人資料保護法》第8條第1項規定，由個人資料保護委員會自資訊通信媒體發展局成員中任命一位主委（Commissioner），如有需要，亦可自資訊通信媒體發展局成員中任命副主委、助理主委及調查員[455]。目前個

---

[453] Singapore, Personal Data Protection Act 2012, Section 9(1), "An individual appointed under section 8(1) or an employee of the Authority, who is authorised in writing by the Chief Executive of the Authority for the purpose of this section, may conduct, with the authorisation of the Public Prosecutor, proceedings in respect of an offence under this Act."

[454] Singapore, Personal Data Protection Act 2012, Section 9(2), "A legal counsel of the Commission who is an advocate and solicitor may — (a) appear in any civil proceedings involving the performance of any function or duty, or the exercise of any power, of the Commission under any written law; and (b) make all applications and do all acts in respect of the civil proceedings on behalf of the Commission or an authorised officer."

[455] Singapore, Personal Data Protection Act 2012, Section 8(1),"The Commission may appoint, by name or office, fromamong public officers and the employees of the Authority —(a) the Commissioner for Personal Data Protection; and(b) such number of Deputy Commissioners for

人資料保護委員會主委（Mr. Tan Kiat How）亦為資訊通信媒體發展局執行長，另有一位副主委（Mr. Yeong Zee Kin）[456]。

(三) 諮詢委員會

依據新加坡《個人資料保護法》第 7 條第 1 項規定，個人資料保護委員會主委得指派一個或多個諮詢委員會，就個人資料保護委員會履行其法定職權事宜提供相關諮詢建議[457]，惟依據同條第 2 項規定，個人資料保護委員會不受前開諮詢委員會之意見拘束[458]。

個人資料保護委員會目前設有一資料保護諮詢委員會（Data Protection Advisory Committee），主席為 Mr. Leong Keng Thai，亦任資訊通信媒體發展局副執行長；本諮詢委員會亦有 13 位成員[459]。

四、法定職務

依據新加坡《個人資料保護法》第 6 條規定，個人資料保護委員會之功能包括[460]：

Personal DataProtection, Assistant Commissioners for Personal DataProtection and inspectors, as the Commission considersnecessary."

[456] PDPC 簡介，網址：https://www.pdpc.gov.sg/about-us/who-we-are，最後到訪日為 106 年 9 月 13 日。

[457] Singapore, Personal Data Protection Act 2012, Section 7(1), "The Minister may appoint one or more advisory committeesto provide advice to the Commission with regard to the performanceof any of its functions under this Act."

[458] Singapore, Personal Data Protection Act 2012, Section 7(2), "The Commission may consult such advisory committees inrelation to the performance of its functions and duties and the exerciseof its powers under this Act but shall not be bound by such consultation."

[459] PDPC 諮詢委員會簡介，網址：https://www.pdpc.gov.sg/about-us/advisory-committee，最後到訪日為 106 年 9 月 13 日。

[460] Singapore, Personal Data Protection Act 2012, Section 6, "The functions of the Commission shall

(一) 於新加坡推廣資料保護之意識；

(二) 提供與資料保護相關之諮詢、建議，及技術、管理或其他專門人員之服務；

(三) 就資料保護事宜向政府提供建議；

(四) 就資料保護事宜於國際間代表新加坡政府；

(五) 從事資料保護相關研究，推廣論壇、工作坊或研討會等教育性活動，並支援其他組織辦理該等活動；

(六) 以個人資料保護委員會或新加坡政府名義，管理與其他組織（包括外國之資料保護主管機關，及國際或政府間組織）間就資料保護事宜進行之技術合作及交流；

(七) 管理、執行《個人資料保護法》；

(八) 履行其他依法賦予個人資料保護委員會之功能；

(九) 辦理、履行經通訊及新聞部長許可，或由部長指派予 PDPC 之其他活動或功能。

(十) 監督權限

另個人資料保護委員會依照《個人資料保護法》相關規定，有下列權限：

1、 發布準則（guidelines）

---

be — (a) to promote awareness of data protection in Singapore; (b) to provide consultancy, advisory, technical, managerial or other specialist services relating to data protection; (c) to advise the Government on all matters relating to data protection; (d) to represent the Government internationally on matters relating to data protection; (e) to conduct research and studies and promote educational activities relating to data protection, including organizing and conducting seminars, workshops and symposia relating thereto, and supporting other organisations conducting such activities; (f) to manage technical co-operation and exchange in the area of data protection with other organisations, including foreign data protection authorities and international or inter‑governmental organisations, on its own behalf or on behalf of the Government; (g) to administer and enforce this Act; (h) to carry out functions conferred on the Commission under any other written law; and (i) to engage in such other activities and perform such functions as the Minister may permit or assign to the Commission by order published in the Gazettei."

新加坡《個人資料保護法》第 49 條規定[461]，個人資料保護委員會得就詮釋個人資料保護法事宜適時發布建議準則，並適時修正或廢止。

2、 發布規範（Regulations）

依據新加坡《個人資料保護法》第 65 條規定[462]，個人資料保護委員會得於達成該法目的之必要範圍內，發布相關規範。

3、 進行審核

---

[461] Singapore, Personal Data Protection Act 2012, Section 49, "(1) The Commission may, from time to time, issue written advisory guidelines indicating the manner in which the Commission will interpret the provisions of this Act. (2) Guidelines issued under this section may, from time to time, be varied, amended or revoked by the Commission. (3) The Commission shall publish the guidelines in any way the Commission thinks fit, but failure to comply with this subsection in respect of any guidelines shall not invalidate the guidelines."

[462] Singapore, Personal Data Protection Act 2012, Section 65, "(1) The Commission may, with the approval of the Minister, make such regulations as may be necessary or expedient for carrying out the purposes and provisions of this Act and for prescribing anything that may be required or authorised to be prescribed by this Act. [Act 22 of 2016 wef 01/10/2016] (2) Without prejudice to the generality of subsection (1), the Commission may, with the approval of the Minister, make regulations for or with respect to all or any of the following matters: (a) [Deleted by Act 22 of 2016 wef 01/10/2016] (b) the form, manner and procedures, relating to the making and responding to requests under section 21 or 22, including the content of responses to such requests, the period for such responses, the circumstances in which an organisation may refuse to provide a response or refuse to confirm or deny the existence of any matter and the fees that an organisation may charge in respect of such requests; (c) the classes of persons who may act under this Act for minors, deceased persons or any other individuals who lack capacity to act under this Act and regulating the manner in which, and the extent to which, any rights or powers of individuals under this Act may be exercised on their behalf;(d) the form, manner and procedures relating to applications and complaints under this Act; (e) the conduct of reviews by the Commission under section 28; (f) the form, manner and procedures for applications for reconsideration by the Commission under section 31, including the fees to be paid in respect of such applications; (g) the form, manner and procedures for appeals to an Appeal Committee, including the fees to be paid in respect of such appeals; (h) the award of costs of or incidental to any proceedings before the Commission or Appeal Committee, and the award of expenses, including any allowances payable to persons in connection with their attendance before the Commission or Appeal Committee; (i) the criteria for determining whether a Singapore telephone number is eligible to be listed in a register; (j) the manner in which entries in the register are to be made, corrected or removed; (k) the manner and form of giving or withdrawing consent for the sending of a specified message; (l) any other matter relating to the establishment, operation or administration of the register; (m) the fees to be paid in respect of applications, and services provided by or on behalf of the Commission, under this Act, including applications to confirm whether a Singapore telephone number is listed in the relevant register for the purposes of section 43(1)(a). [Act 22 of 2016 wef 01/10/2016] (3) Regulations made under this section may provide differently for different organisations, individuals, classes of organisations or classes of individuals."

新加坡《個人資料保護法》第 28 條規定[463]，針對機關團體拒絕提供或拒絕更正申訴人之個資、超過合理時間仍未提供或更正等情事，個人資料保護委員會得確認或推翻該等拒絕提供或拒絕更正之決定；另針對機關團體向申訴人就取得或更正個資收取之費用，個人資料保護委員會亦得等進行審核，並得確認、減少或禁止該等費用，或要求該等機關團體退費予申訴人。

4、 提出要求（Power to give directions）與裁罰

依據新加坡《個人資料保護法》第 29 條[464]，如機

---

[463] Singapore, Personal Data Protection Act 2012, Section 28,"(1) On the application of a complainant, the Commission may review — (a) a refusal to provide access to personal data requested by the complainant under section 21, or a failure to provide such access within a reasonable time; (b) a fee required from the complainant by an organisation in relation to a request by the complainant under section 21 or 22; or (c) a refusal to correct personal data in accordance with a request by the complainant under section 22, or a failure to make such correction within a reasonable time. (2) Upon completion of its review under subsection (1), the Commission may — (a) confirm the refusal to provide access to the personal data, or direct the organisation to provide access to the personal data, within such time as the Commission may specify; (b) confirm, reduce or disallow a fee, or direct the organisation to make a refund to the complainant; or (c) confirm the refusal to correct the personal data, or direct the organisation to correct the personal data, in such manner and within such time as the Commission may specify."

[464] Singapore, Personal Data Protection Act 2012, Section 29, "(1) The Commission may, if it is satisfied that an organisation is not complying with any provision in Parts III to VI, give the organisation such directions as the Commission thinks fit in the circumstances to ensure compliance with that provision. (2) Without prejudice to the generality of subsection (1), the Commission may, if it thinks fit in the circumstances to ensure compliance with Parts III to VI, give the organisation all or any of the following directions:(a) to stop collecting, using or disclosing personal data in contravention of this Act;(b) to destroy personal data collected in contravention of this Act; (c) to comply with any direction of the Commission under section 28(2); (d) to pay a financial penalty of such amount not exceeding $1 million as the Commission thinks fit.(3) Subsection (2)(d) shall not apply in relation to any failure to comply with a provision of this Act, the breach of which is an offence under this Act. (4) The Commission shall, in any direction requiring the payment of a financial penalty, specify the date before which the financial penalty is to be paid, being a date not earlier than the end of the period within which an application for reconsideration of the direction, or an appeal against the direction, may be brought under section 31 or 34, respectively. (5) The interest payable on the outstanding amount of any financial penalty imposed under subsection (2)(d) and for payment by instalment (as may be directed by the Commission in its discretion) of any financial penalty imposed under subsection (2)(d) shall be at such rate as the Commission may direct, which shall not exceed the rate prescribed in the Rules of Court in respect of judgment debts. (6) Any interest ordered to be paid under subsection (5) shall form part of the penalty payable and be

關團體未遵守該法第11至第26條有關個資保護之一般性規範、個資之蒐集、利用、揭露、取得、更正及維護等規定，個人資料保護委員會得對該等機關團體提出要求，強制其停止相關個資蒐集、利用或揭露等行為、銷毀違法蒐集之個資，或對其裁罰 100 萬新幣以下之罰鍰等；且該等要求可由新加坡法院強制執行。又個人資料保護委員會針對違反新加坡個資保護法中「謝絕來電（Do Not Call）」規定者，有權進行調查及處罰裁定，並交由法院執行[465]。

5、 進行調查（Power to investigate）

同法第 50 條規定[466]，個人資料保護委員會及其下

---

enforced in accordance with section 30."

[465] Singapore, Personal Data Protection Act, Part VII, Sec. 30, "(1) For the purposes of enforcement of any direction made by the Commission under section 28(2) or 29, the Commission may apply for the direction to be registered in a District Court in accordance with the Rules of Court and the District Court shall register the direction in accordance with the Rules of Court. (2) From the date of registration of any direction under subsection (1), the direction shall be of the same force and effect, and all proceedings may be taken on the direction, for the purposes of enforcement as if it had been an order originally obtained in the District Court which shall have power to enforce it accordingly. (3) A District Court shall have jurisdiction to enforce any direction in accordance with subsection (2) regardless of the monetary amount involved and may, for the purpose of enforcing such direction, make any order — (a) to secure compliance with the direction; or (b) to require any person to do anything to remedy, mitigate or eliminate any effects arising from — (i) anything done which ought not, under the direction, to have been done; or (ii) anything not done which ought, under the direction, to have been done, which would not have occurred had the direction been complied with".

[466] Singapore, Personal Data Protection Act 2012, Section 50, "(1) The Commission may, upon complaint or of its own motion, conduct an investigation under this section to determine whether an organisation is not complying with this Act. (2) The powers of investigation under this section of the Commission and the inspectors shall be as set out in the Ninth Schedule. (3) The Commission may suspend, discontinue or refuse to conduct an investigation under this section if it thinks fit, including but not limited to any of the following circumstances:(a) the complainant has not complied with a direction under section 27(2); (b) the parties involved in the matter have mutually agreed to settle the matter; (c) any party involved in the matter has commenced legal proceedings against another party in respect of any contravention or alleged contravention of this Act by the other party; (d) the Commission is of the opinion that the matter may be more appropriately investigated by another regulatory authority and has referred the matter to that authority; or (e) the Commission is of the opinion that — (i) a complaint is frivolous or vexatious or is not made in good faith; or (ii) any other circumstances warrant refusing to conduct, suspending or discontinuing the investigation. (4) An organisation shall retain records relating to an investigation under this

之調查員，得依據申訴案或主動調查機關團體是否確實遵守該法規定，亦得裁量申訴案是否為惡意申訴或濫訴，以決定是否受理、暫停或終止調查。

同法附表 9（Ninth Schedule）另明定前述調查權之執行細節：第 1 段規定個人資料保護委員會及其調查員為進行調查，得以書面方式要求機關團體提供與調查相關之特定文件或資訊[467]；第 2 段則規定[468]，於調

---

section for one year after the conclusion of the investigation or any longer period specified in writing by the Commission."

[467] Singapore, Personal Data Protection Act 2012, Ninth Schedule, Paragraph 1,"(1) For the purposes of an investigation under section 50, the Commission or an inspector may, by notice in writing to any organisation, require the organization to produce to the Commission or the inspector a specified document or specified information, which the Commission or inspector considers relates to any matter relevant to such investigation. (2) A notice under sub-paragraph (1) shall indicate the purpose for which the specified document or specified information is required by the Commission. (3) The Commission may specify in the notice — (a) the time and place at which any document is to be produced or any information is to be provided; and (b) the manner and form in which it is to be produced or provided. (4) The power under this paragraph to require an organisation to produce a document includes the power — (a) if the document is produced — (i) to take copies of it or extracts from it; and (ii) to require such organisation, or any person who is a present or past officer of the organisation, or is or was at any time employed by the organisation, to provide an explanation of the document; or (b) if the document is not produced, to require such organisation or person to state, to the best of his knowledge and belief, where it is. (5) In sub-paragraphs (1) and (2), "specified" means — (a) specified or described in the notice; or (b) falling within a category which is specified or described in the notice."

[468] Singapore, Personal Data Protection Act 2012, Ninth Schedule, Paragraph 2,"(1) In connection with an investigation under section 50, an inspector, and such other persons as the inspector may require to assist him, may enter any premises. (2) No inspector or person assisting the inspector shall enter any premises in exercise of the powers under this paragraph unless the inspector has given the occupier of the premises a written notice which — (a) gives at least 2 working days' notice of the intended entry; and (b) indicates the subject-matter and purpose of the investigation. (3) Sub-paragraph (2) shall not apply if the inspector has reasonable grounds for suspecting that the premises are, or have been, occupied by an organisation which is being investigated in relation to a contravention of this Act and if the inspectorhas taken all such steps as are reasonably practicable to give written notice under that sub-paragraph but has not been able to do so. (4) Where sub-paragraph (3) applies, the power of entry conferred by sub-paragraph (1) shall be exercised upon production of — (a) evidence of the inspector's appointment; and (b) a document containing the information referred to in sub-paragraph (2)(b). (5) An inspector or a person assisting the inspector entering any premises under this paragraph may — (a) take with him such equipment as appears to him to be necessary; (b) require any person on the premises — (i) to produce any document which he considers relates to any matter relevant to the investigation; and (ii) if the document is produced, to provide an explanation of it; (c) require any person to state, to the best of the person's knowledge and belief, where any such document is to be found; (d) take copies of, or extracts from, any document which is produced; (e) require any information which is stored in any electronic form and is accessible from the premises and which he considers relates to any matter

查相關之範圍內，調查員可於2工作天內前提出通知將調查之主旨及目的告知任何地產建物之使用人後，即可進入該地產或建物；另，如調查員合理懷疑該地產或建物刻正或曾經由與個人資料保護法違法行為調查相關之機關團體所使用，且於合理範圍內已盡一切努力仍無法通知使用人，則調查員出示相關證明文件即可逕行進入該地產或建物。

如個人資料保護委員會或其調查員循前述方式均無法取得所需文件、合理懷疑依其職權可要求取得之文件可能遭隱匿、移動、竄改或銷毀，則依據附表第3段規定[469]，可向法院申請搜索令，授權調查員可強制進

---

relevant to the investigation, to be produced in a form — (i) in which it can be taken away; and (ii) in which it is visible and legible; and (f) take any step which appears to be necessary for the purpose of preserving or preventing interference with any document which he considers relates to any matter relevant to the investigation."

[469] Singapore, Personal Data Protection Act 2012, Ninth Schedule, Paragraph 3,"(1) The Commission or any inspector may apply to a court for a warrant and the court may issue such a warrant if it is satisfied that — (a) there are reasonable grounds for suspecting that there are, on any premises, documents — (i) the production of which has been required under paragraph 1 or 2; and (ii) which have not been produced as required;(b) there are reasonable grounds for suspecting that — (i) there are, on any premises, documents which the Commission or the inspector has power under paragraph 1 to require to be produced; and (ii) if the documents were required to be produced, they would not be produced but would be concealed, removed, tampered with or destroyed; or (c) an inspector or a person assisting the inspector has attempted to enter the premises in the exercise of his powers under paragraph 2 but has been unable to do so and that there are reasonable grounds for suspecting that there are, on the premises, documents the production of which could have been required under that paragraph. (2) Awarrant under this paragraph shall authorise a named officer, and such other persons as the inspector may require to assist him, to do all or any of the following: (a) to enter the premises specified in the warrant, using such force as is reasonably necessary for the purpose; (b) to search any person on those premises if there are reasonable grounds for believing that that person has in his possession any document, equipment or article which has a bearing on the investigation; (c) to search the premises and take copies of, or extracts from, any document appearing to be of a kind in respect of which the application under sub-paragraph (1) was granted (the relevant kind); (d) to take possession of any document appearing to be of the relevant kind if — (i) such action appears to be necessary for preserving the document or preventing interference with it; or (ii) it is not reasonably practicable to take copies of the document on the premises; (e) to take any other step which appears to be necessary for the purpose mentioned in sub-paragraph (d)(i); (f) to require any person to provide an explanation of any document appearing to be of the relevant kind or to state, to the best of his knowledge and belief, where it may be found; (g) to require any information which is stored in any electronic form and is accessible from the premises and which he considers relates to

any matter relevant to the investigation, to be produced in a form —(b) there are reasonable grounds for suspecting that — (i) there are, on any premises, documents which the Commission or the inspector has power under paragraph 1 to require to be produced; and (ii) if the documents were required to be produced, they would not be produced but would be concealed, removed, tampered with or destroyed; or (c) an inspector or a person assisting the inspector has attempted to enter the premises in the exercise of his powers under paragraph 2 but has been unable to do so and that there are reasonable grounds for suspecting that there are, on the premises, documents the production of which could have been required under that paragraph. (2) Awarrant under this paragraph shall authorise a named officer, and such other persons as the inspector may require to assist him, to do all or any of the following: (a) to enter the premises specified in the warrant, using such force as is reasonably necessary for the purpose; (b) to search any person on those premises if there are reasonable grounds for believing that that person has in his possession any document, equipment or article which has a bearing on the investigation; (c) to search the premises and take copies of, or extracts from, any document appearing to be of a kind in respect of which the application under sub-paragraph (1) was granted (the relevant kind); (d) to take possession of any document appearing to be of the relevant kind if — (i) such action appears to be necessary for preserving the document or preventing interference with it; or (ii) it is not reasonably practicable to take copies of the document on the premises; (e) to take any other step which appears to be necessary for the purpose mentioned in sub-paragraph (d)(i); (f) to require any person to provide an explanation of any document appearing to be of the relevant kind or to state, to the best of his knowledge and belief, where it may be found; (g) to require any information which is stored in any electronic form and is accessible from the premises and which he considers relates to any matter relevant to the investigation, to be produced in a form —(i) in which it can be taken away; or (ii) in which it is visible and legible; and (h) to remove from those premises for examination any equipment or article which relates to any matter relevant to the investigation. (3) If, in the case of a warrant under sub-paragraph (1)(b), the court is satisfied that it is reasonable to suspect that there are also on the premises other documents relating to the investigation concerned, the warrant shall also authorise the actions mentioned in sub-paragraph (2) to be taken in relation to any such document. (4) Where possession of any document is taken under sub-paragraph (2)(d) or (3), the named officer may, at the request of the person from whom possession of the document was taken, provide such person with a copy of the document. (5) A named officer may allow any equipment or article which has a bearing on an investigation and which may be removed from any premises for examination under sub-paragraph (2)(h) to be retained on those premises subject to such conditions as the named officer may require. (6) A warrant issued under this paragraph shall — (a) indicate the subject-matter and purpose of the investigation; and (b) continue in force until the end of the period of one month beginning from the day on which it is issued. (7) The powers conferred by this paragraph shall not be exercised except upon production of a warrant issued under this paragraph. (8) Any person entering any premises by virtue of a warrant under this paragraph may take with him such equipment as appears to him to be necessary. (9) If there is no one at the premises when the named officer proposes to execute such a warrant, he shall, before executing it — (a) take such steps as are reasonable in all the circumstances to inform the occupier of the intended entry; and (b) if the occupier is informed, afford him or his legal or other representative a reasonable opportunity to be present when the warrant is executed. (10) If the named officer is unable to inform the occupier of the intended entry, he shall, when executing the warrant, leave a copy of the warrant in a prominent place on the premises. (11) On leaving any premises which he has entered by virtue of a warrant under this paragraph, the named officer shall, if the premises are unoccupied or the occupier is temporarily absent, leave them as effectively secured as he found them.(12) Any document of which possession is taken under sub-paragraph (2)(d) or (3) may be retained for a period of not more than 3 months. (13) In this paragraph — “named officer” means an inspector named in the warrant; “occupier”, in relation to any premises, means a person whom the inspector reasonably believes is the occupier of those premises.”

員會或其調查員行使職權，或蓄意提供錯誤、誤導之資訊者，依第 51 條第 5 項規定[470]，個人得處新幣一萬元以下之罰金或 12 個月以下之有期徒刑(或兩者併行)，非個人則得處新幣十萬元以下之罰金。

[470] Singapore, Personal Data Protection Act 2012,Section 51(5), "An organisation or person that commits an offence under subsection (3)(b) or (c) is liable — (a) in the case of an individual, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both; and (b) in any other case, to a fine not exceeding $100,000."

第九節　馬來西亞—個人資料保護署（JPDP）

一、概述

馬來西亞個人資料保護署（JPDP）係該國國會通過 2009 年《個人資料保護法案（Personal Data Protection Bill 2009）》後，於 2011 年 5 月 16 日成立，隸屬通訊暨多媒體部（相當於我國三級機關），以執行 2010 年《個人資料保護法（Personal Data Protection Act 2010）》為職責，並以商業交易中個人資料之處理，及避免個人資料濫用為規範重點。個人資料保護署由署長兼個資保護委員（Director General cum Commissioner）領導，其三個主要下屬單位為：註冊及營運處（Registration and Operation Division）、監督處（Monitoring Division）及法務處（Legal Division）。

《個人資料保護法》第 51 條授權個資保護委員指派必要之人員[471]，襄助其執行職務及發揮職權。

二、監管對象與主管法規

馬來西亞個人資料保護署專責《個人資料保護法》之監管，且該法僅適用於非公務機關[472]。

三、組織規範

(一)正副首長

---

[471] Malaysia, Personal Data Protection Act 2010, Section 51, “The Commissioner may employ on such terms and conditions as he thinks desirable such officers and servants as may be necessary to assist him in the performance of his functions and the exercise of his powers under this Act.”

[472] Malaysia, Personal Data Protection Act 2010, Section3(1), “This Act shall not apply to the Federal Government and State Governments”.

《個人資料保護法》第 47 條第 1 項規定[473]，個資保護委員由部長（指通訊暨多媒體部長）指派，其任期依同法第 53 條規定[474]以 3 年為限，但得續任，委員待遇則依同法第 57 條規定[475]，由部長與財政部長商議後訂定。部長可依《個人資料保護法》第 54 條第 1 項規定[476]免除委員之職務，委員亦得依同條第 2 項規定[477]，提前兩週時間以書面向部長請辭；《個人資料保護法》第 56 條另規定[478]委員除被免職或請辭獲准外，於下列情況下即自動去職：

1、身故；

2、經判決詐欺、不誠實、道德敗壞、貪瀆或其他刑罰為兩年以上有期徒刑之罪名確定；

3、行為損及個資保護委員一職之信譽；

---

[473] Malaysia, Personal Data Protection Act 2010, Section 47(1), "The Minister shall appoint any person as the "Personal Data Protection Commissioner" for the purposes of carrying out the functions and powers assigned to the Commissioner under this Act on such terms and conditions as he thinks desirable."

[474] Malaysia, Personal Data Protection Act 2010, Section 53, "Subject to such conditions as may be specified in his instrument of appointment, the Commissioner shall, unless he sooner resigns or vacates his office or his appointment is sooner revoked, hold office for a term not exceeding three years and may be eligible for reappointment."

[475] Malaysia, Personal Data Protection Act 2010, Section 57, "The Commissioner shall be paid such remuneration and allowances as the Minister may determine after consultation with the Minister of Finance."

[476] Malaysia, Personal Data Protection Act 2010, Section 54(1), "The Minister may at any time revoke the appointment of the Commissioner and shall state the reason for such revocation."

[477] Malaysia, Personal Data Protection Act 2010, Section 54(2), "The Commissioner may at any time resign his office by giving a written notice addressed to the Minister fourteen days prior to the intended date of resignation."

[478] Malaysia, Personal Data Protection Act 2010, Section 56, "The office of the Commissioner shall be vacated— (a) if he dies; (b) if there has been proved against him, or he has been convicted of, a charge in respect of—(i) an offence involving fraud, dishonesty or moral turpitude; (ii) an offence under any law relating to corruption; or (iii) any other offence punishable with imprisonment (in itself only or in addition to or in lieu of a fine) for more than two years; (c) if his conduct, whether in connection with his duties as a Commissioner or otherwise, has been such as to bring discredit on the office of the Commissioner; (d) if he becomes bankrupt; (e) if he is of unsound mind or is otherwise incapable of discharging his duties; (f) if his appointment is revoked by the Minister; or (g) if his resignation is accepted by the Minister."

4、破產；

5、心智狀況無法執行職務。

依據《個人資料保護法》第 50 條規定[479]，副個資保護委員及助理個資保護委員由委員指派，人數、任期、待遇亦由個資保護委員經部長同意後決定。委員可依同法第 58 條規定[480]，將其於《個人資料保護法》下之職務及職權指派予副個資保護委員及助理個資保護委員代行，委員去職或因故暫時無法視事時，部長亦可依該法第 55 條規定[481]，指定一位副個資保護委員暫代委員職務。

(二)地位

《個人資料保護法》第 47 條第 3 項[482]規定，個資保護

---

[479] Malaysia, Personal Data Protection Act 2010, Section 50, "(1) The Commissioner may, with the approval of the Minister, from time to time, appoint such number of public officers as Deputy Commissioners and such number of persons as Assistant Commissioners as are necessary to assist the Commissioner in the performance of his functions and the exercise of his powers under this Act. (2) The Deputy Commissioners and Assistant Commissioners appointed under subsection (1) shall hold office for such periods, receive such remuneration, allowances or benefits, and shall be subject to such terms and conditions of service as the Commissioner, with the approval of the Minister, may determine. (3) The Deputy Commissioners and Assistant Commissioners appointed under subsection (1) shall be subject to the supervision, direction and control of the Commissioner."

[480] Malaysia, Personal Data Protection Act 2010, Section 58, "(1) The Commissioner may, subject to such conditions, limitations or restrictions as he may think fit to impose, delegate any of his functions or powers imposed or conferred upon him under this Act, except his power of delegation, to the Deputy Commissioners or Assistant Commissioners, and any function or power so delegated may be performed and exercised by the officer in the name and on behalf of the Commissioner. (2) The delegation under subsection (1) shall not preclude the Commissioner himself from performing or exercising at any time the delegated functions or powers."

[481] Malaysia, Personal Data Protection Act 2010, Section 55, "(1) The Minister may temporarily appoint a Deputy Commissioner to perform the functions and powers of the Commissioner for the period when—(a) the Commissioner is by reason of illness, leave of absence or any other cause unable to perform his functions for any substantial period; or (b) the office of the Commissioner is vacant. (2) A person appointed under subsection (1) shall, during the period in which he is performing the functions and exercising the powers of the Commissioner under this section, be deemed to be the Commissioner."

[482] Malaysia, Personal Data Protection Act 2010, Section 47(3), "The Commissioner appointed under subsection (1) shall be a body corporate having perpetual succession and a common seal."

委員為永久存續之法人（body corporate）；同法第 59 條[483]則規定委員應對部長負責，接受並貫徹部長之指示。

(三)組織架構

個人資料保護署由正副署長(Director、Deputy Director）領導運作，其中署長係由個資保護委員兼任，下轄之主要單位包括監督處、註冊及營運處及法務處，其職責分述如下：

1、監督處

該處負責針對各機關遵循《個人資料保護法》之情形進行評量、調查及監督。

2、註冊及營運處

該處負責協調、監督個資使用者登記相關事宜，包括管理、更新及撤銷登記資料、核發登記證明等；另該處亦負責管理研擬各級個資使用者實務準則之「使用者論壇（Data User Forum）」運作事宜。

3、法務處

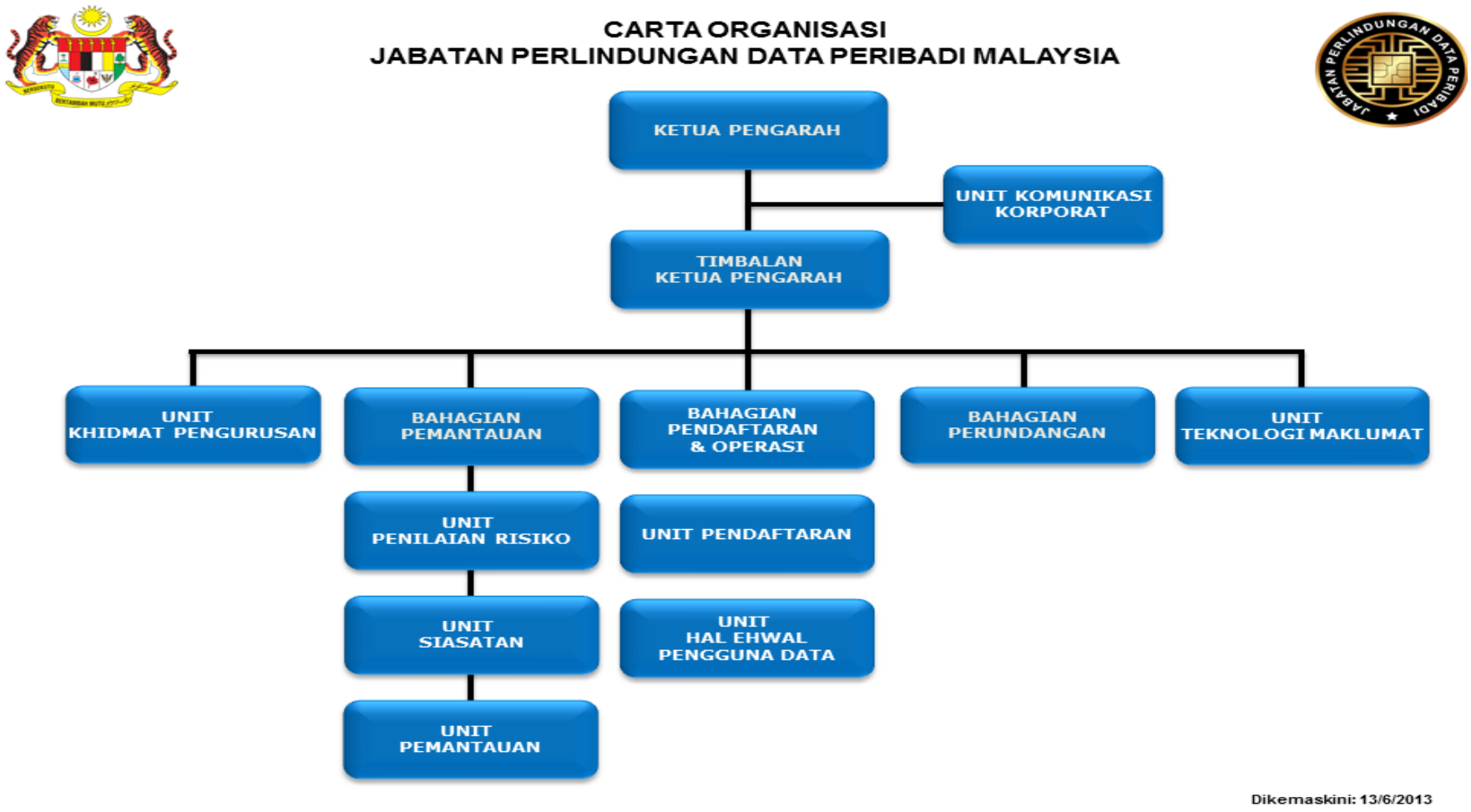
該處負責提供法律意見、撰擬法規草案、檢視法律文件、辦理裁罰事宜，並於民事訴訟中代表個人資料保護署。

個人資料保護署另設聯絡組（Corporate Communications

[483] Malaysia, Personal Data Protection Act 2010, Section 59, "(1) The Commissioner shall be responsible to the Minister. (2) The Minister may give to the Commissioner directions of a general character consistent with the provisions of this Act relating to the performance of the functions and powers of the Commissioner and the Commissioner shall give effect to such directions."

Unit）、資訊科技組（Information Technology Unit）及管理服務組（Management Services Unit），分別負責對外宣導、管理個人資料保護署內部資訊系統及個資使用者登記系統,及管理個人資料保護署人事、會計、檔案等事宜。

圖 6 馬來西亞個人資料保護署組織架構圖



四、法定職務

個資保護委員之職責及職權，分別規定於《個人資料保護法》第 48[484]及第 49 條[485]，分述如下：

(一) 職責

1、就國家之個資保護政策及其他所有相關事宜向部長提供諮詢意見；

2、以訂定施行細則、程序等方式，執行個資保護法規；

---

[484] Malaysia, Personal Data Protection Act 2010, Section 48, "The Commissioner shall have the following functions: (a) to advise the Minister on the national policy for personal data protection and all other related matters; (b) to implement and enforce the personal data protection laws, including the formulation of operational policies and procedures; (c) to promote and encourage associations or bodies representing data users to prepare codes of practice and to disseminate to their members the codes of practice for the purposes of this Act; (d) to cooperate with bodies corporate or government agencies for the purpose of performing his functions; (e) to determine in pursuance of section 129 whether any place outside Malaysia has in place a system for the protection of personal data that is substantially similar to that as provided for under this Act or that serves the same purposes as this Act; (f) to undertake or cause to be undertaken research into and monitor developments in the processing of personal data, including technology, in order to take account any effects such developments may have on the privacy of individuals in relation to their personal data; (g) to monitor and supervise compliance with the provisions of this Act, including the issuance of circulars, enforcement notices or any other instruments to any person; (h) to promote awareness and dissemination of information to the public about the operation of this Act; (i) to liaise and cooperate with persons performing similar personal data protection functions in any place outside Malaysia in respect of matters of mutual interest, including matters concerning the privacy of individuals in relation to their personal data; (j) to represent Malaysia through participation in events that relate to personal data protection as authorized by the Minister, whether within or outside Malaysia; and (k) to carry out such activities and do such things as are necessary, advantageous and proper for the administration of this Act, or such other purposes consistent with this Act as may be directed by the Minister."

[485] Malaysia, Personal Data Protection Act 2010, Section 49, "(1) The Commissioner shall have all such powers to do all things necessary or expedient for or in connection with the performance of his functions under this Act. (2) Without prejudice to the generality of subsection (1), the powers of the Commissioner shall include the power—(a) to collect such fees as may be prescribed by the Minister; (b) to appoint such agents, experts, consultants or any other persons as he thinks fit to assist him in the performance of his functions; (c) to formulate human resource development and cooperation programmes for the proper and effective performance of his functions; (d) to enter into contracts; (e) to acquire, purchase, take, hold and enjoy any movable or immovable property of every description for the performance of his functions, and to convey, assign, surrender, yield up, charge, mortgage, demise, transfer or otherwise dispose of, or deal with such property or any interest therein vested in him; (f) to perform such other functions as the Minister may assign from time to time; and (g) to do all such things as may be incidental to or consequential upon the performance of his functions."

3、促進個資使用者之公協會等組織研擬實務準則，並提供予該等組織之成員；

4、就執行其職務事宜與政府部門或相關公法人合作；

5、依據《個人資料保護法》第 129 條[486]規定，就馬來西亞境外之地點是否具有與《個人資料保護法》目的相同且實質內容相近之個資保護體制，向部長提供建議；

6、留意個資處理技術等相關事宜發展並進行研究，以將該等發展對個資隱私之影響納入施政考量；

7、透過通函及強制執行通知書（enforcement notices）等方

[486] Malaysia, Personal Data Protection Act 2010, Section 129, "(1) A data user shall not transfer any personal data of a data subject to a place outside Malaysia unless to such place as specified by the Minister, upon the recommendation of the Commissioner, by notification published in the Gazette. (2) For the purposes of subsection (1), the Minister may specify any place outside Malaysia if—(a) there is in that place in force any law which is substantially similar to this Act, or that serves the same purposes as this Act; or (b) that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by this Act. (3) Notwithstanding subsection (1), a data user may transfer any personal data to a place outside Malaysia if—(a) the data subject has given his consent to the transfer; (b) the transfer is necessary for the performance of a contract between the data subject and the data user; (c) the transfer is necessary for the conclusion or performance of a contract between the data user and a third party which—(i) is entered into at the request of the data subject; or (ii) is in the interests of the data subject; (d) the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights; (e) the data user has reasonable grounds for believing that in all circumstances of the case—(i) the transfer is for the avoidance or mitigation of adverse action against the data subject; (ii) it is not practicable to obtain the consent in writing of the data subject to that transfer; and (iii) if it was practicable to obtain such consent, the data subject would have given his consent; (f) the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of this Act; (g) the transfer is necessary in order to protect the vital interests of the data subject; or (h) the transfer is necessary as being in the public interest in circumstances as determined by the Minister. (4) Where the Commissioner has reasonable grounds for believing that in a place as specified under subsection (1) there is no longer in force any law which is substantially similar to this Act, or that serves the same purposes as this Act— (a) the Commissioner shall make such recommendations to the Minister who shall, either by cancelling or amending the notification made under subsection (1), cause that place to cease to be a place to which personal data may be transferred under this section; and (b) the data user shall cease to transfer any personal data of a data subject to such place with effect from the time as specified by the Minister in the notification. (5) A data user who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both. (6) For the purposes of this section, "adverse action", in relation to a data subject, means any action that may adversely affect the data subject's rights, benefits, privileges, obligations or interests."

式，監督各機關遵循《個人資料保護法》情形；

8、促進公眾對《個人資料保護法》運作之瞭解；

9、與馬來西亞境外之個資保護機關，就雙方具共同利益事宜（如個資隱私）進行合作；

10、依部長授權，於國內外個資保護相關活動中代表馬來西亞；

11、依部長指示，辦理執行本法之其他相關事宜。

(二) 職權

1、辦理執行本法之其他相關事宜。

2、收取部長訂定之規費；

3、指派幹員、專家、顧問及其他可協助其執行職務之人員；

4、研擬人力資源發展及合作計畫，以有效執行其職務；

5、訂定合約；

6、為執行其職務所需，取得及處理各類動產及不動產；

7、執行部長交辦之其他職務；

8、處理因其職務產生之其他事宜。

第十節　菲律賓—國家隱私委員會（NPC）

一、概述

為保障隱私權、確保個人資料自由流通與創新應用，並確保政府以及民間企業持有之個人資料受到適當的保護[487]，菲律賓政府於 2011 年 7 月通過《資料隱私法（Data Privacy Act of 2012）》，正式設置菲律賓國家隱私委員會（National Privacy Commission，以下簡稱國家隱私委員會），負責管理公務機關與非公務機關蒐集、處理及利用個人資料等相關問題[488]。

二、監管對象與主管法規

菲律賓國家隱私委員會主管《資料隱私法》，對公務機關有監督其是否遵守《資料隱私法》之權力，以確保其資訊安全及技術措施達到個人資料保護的最低標準，必要時並建議其採取必要的措施[489]；但對非公務機關僅有要求其制定並實施個資保護措施之權力。

此外，國家隱私委員會並無裁罰之權，僅能向法務部建議對違法者起訴及施以處罰[490]。

---

487 Philippines, Data Privacy Act of 2012, Section 2, "Declaration of Policy. – It is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected".

488 Philippines, Data Privacy Act of 2012, Legislative description。

489 Philippines, Data Privacy Act of 2012, Section 7(e), "Monitor the compliance of other government agencies or instrumentalities on their security and technical measures and recommend the necessary action in order to meet minimum standards for protection of personal information pursuant to this Act".

490 Philippines, Data Privacy Act of 2012, Section 7(i), "Recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sections 25 to 29 of this Act".

三、組織規範

(一) 地位及任免

依據《資料隱私法》，國家隱私委員會隸屬於菲律賓國家資通訊技術部（Department of Information and Communications Technology，以下簡稱 DICT），設置隱私保護委員（Privacy Commissioner）一名擔任國家隱私委員會主席、副隱私保護委員（Deputy Privacy Commissioners）兩名，分別負責資料處理系統以及政策規劃。隱私保護委員及副隱私保護委員由總統任命，任期三年，得連任一次，若遇有出缺，其遞補方式亦同[491]。

(二) 隱私保護委員資格與待遇

隱私保護委員必須至少 35 歲以上，且具有良好的道德品格、公眾評價，以及是資訊技術和個人資料保護隱私領域公認的專家，並享有相當於部長（Secretary）職級的福利、待遇和薪酬[492]；副隱私保護委員必須是資訊技術和個人資料保護隱私領域公認的專家，並享有相當於次長

---

[491] Philippines, Data Privacy Act of 2012, Section 9.(1), "Organizational Structure of the Commission. – The Commission shall be attached to the Department of Information and Communications Technology (DICT) and shall be headed by a Privacy Commissioner, who shall also act as Chairman of the Commission. The Privacy Commissioner shall be assisted by two (2) Deputy Privacy Commissioners, one to be responsible for Data Processing Systems and one to be responsible for Policies and Planning. The Privacy Commissioner and the two (2) Deputy Privacy Commissioners shall be appointed by the President of the Philippines for a term of three (3) years, and may be reappointed for another term of three (3) years. Vacancies in the Commission shall be filled in the same manner in which the original appointment was made".

[492] Philippines, Data Privacy Act of 2012, Section 9.(2), "The Privacy Commissioner must be at least thirty-five (35) years of age and of good moral character, unquestionable integrity and known probity, and a recognized expert in the field of information technology and data privacy. The Privacy Commissioner shall enjoy the benefits, privileges and emoluments equivalent to the rank of Secretary".

（Undersecretary）職級的福利、待遇和薪酬[493]。

(三) 隱私保護委員行為責任範圍

隱私保護委員、副隱私保護委員或其他依其指示之人，依法執行本委員會之職務時，不對其所為之行為負任何民事履行、損害賠償之責；但對其違反法令、公共政策或善良風俗之故意或過失行為負責，即使是依照上級指示所為。上述之人在合法履行其職責的情況下，面臨訴訟時，委員會應償還其訴訟的合理費用[494]。

(四) 內部組織與成員

國家隱私委員會得成立秘書處，秘書處之主要工作人員必須在政府機關處理個人資料以及隱私保護相關業務至少5年以上[495]。

(五) 預算與帳目

---

493 Philippines, Data Privacy Act of 2012, Section 9.(3), "The Deputy Privacy Commissioners must be recognized experts in the field of information and communications technology and data privacy. They shall enjoy the benefits, privileges and emoluments equivalent to the rank of Undersecretary".

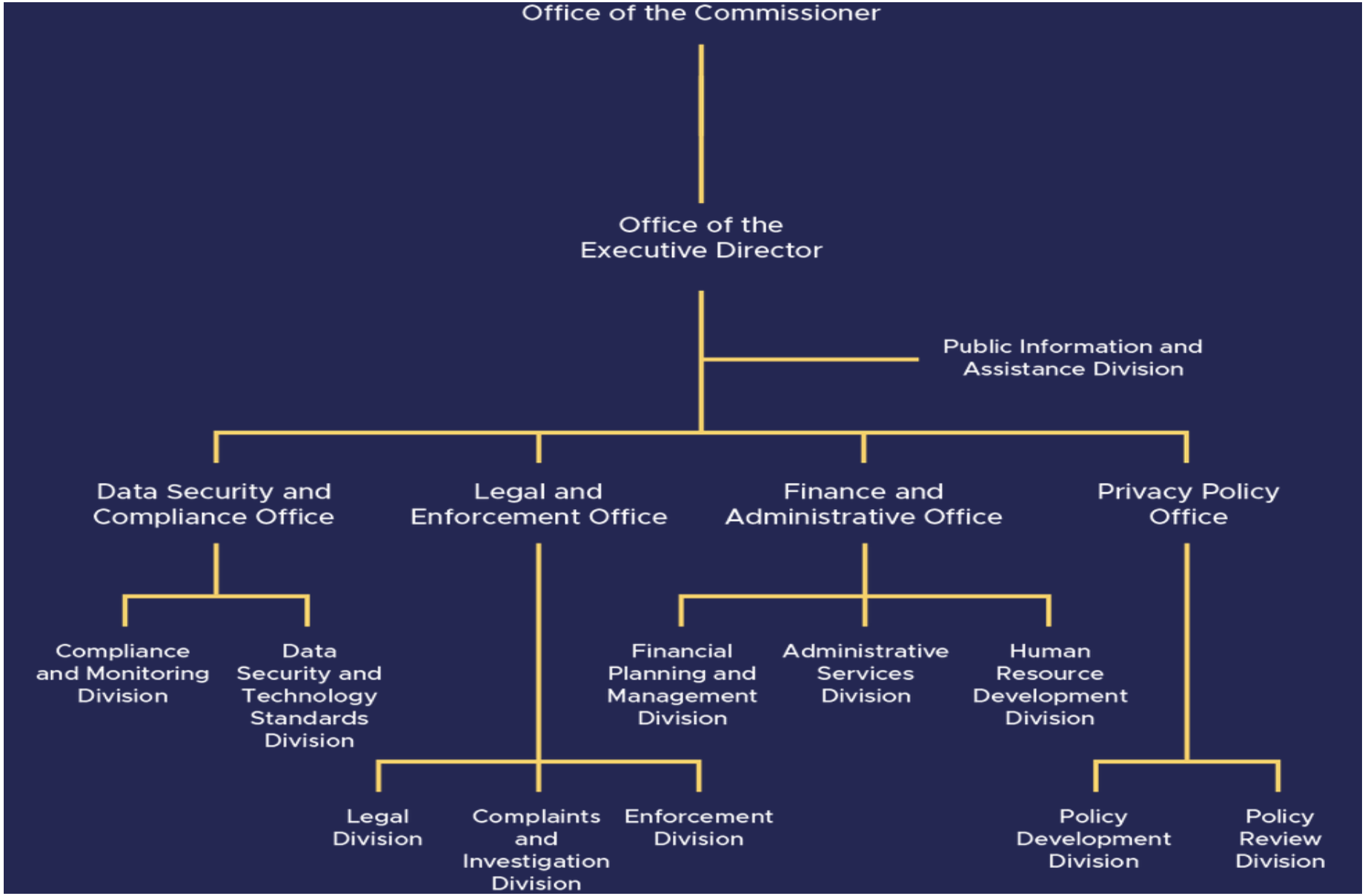
494 Philippines, Data Privacy Act of 2012, Section 9.(4), "The Privacy Commissioner, the Deputy Commissioners, or any person acting on their behalf or under their direction, shall not be civilly liable for acts done in good faith in the performance of their duties. However, he or she shall be liable for willful or negligent acts done by him or her which are contrary to law, morals, public policy and good customs even if he or she acted under orders or instructions of superiors: Provided, That in case a lawsuit is filed against such official on the subject of the performance of his or her duties, where such performance is lawful, he or she shall be reimbursed by the Commission for reasonable costs of litigation".

495 Philippines, Data Privacy Act of 2012, Section 9.(5), "The Secretariat. – The Commission is hereby authorized to establish a Secretariat. Majority of the members of the Secretariat must have served for at least five (5) years in any agency of the government that is involved in the processing of personal information including, but not limited to, the following offices: Social Security System (SSS), Government Service Insurance System (GSIS), Land Transportation Office (LTO), Bureau of Internal Revenue (BIR), Philippine Health Insurance Corporation (PhilHealth), Commission on Elections (COMELEC), Department of Foreign Affairs (DFA), Department of Justice (DOJ), and Philippine Postal Corporation (Philpost)".

國家隱私委員會之法定年度起始預算為 2000 萬比索（約新台幣 1200 萬元），其後五年內年度預算應包含於未來每年之政府年度預算中，為 1000 萬比索（約新台幣 600 萬元）[496]。

[496] Philippines, Data Privacy Act of 2012, Section 41, "Appropriations Clause. – The Commission shall be provided with an initial appropriation of Twenty million pesos (Php20,000,000.00) to be drawn from the national government. Appropriations for the succeeding years shall be included in the General Appropriations Act. It shall likewise receive Ten million pesos (Php10,000,000.00) per year for five (5) years upon implementation of this Act drawn from the national government".

圖 7 菲律賓國家隱私委員會組織架構圖



四、法定職務

國家隱私委員會負責《資料隱私法》之實施以及落實，監督並確保行政機關遵守為隱私保護、個人資料保護所制定之國際標準，該委員會應具有以下功能：

(一) 確保個人資料持有者遵循《資料隱私法》[497]。

(二) 針對個人資料或隱私侵犯案件，國家隱私委員會應接受投訴、進行調查，並提供方便並迅速解決爭議之解決程序，對影響任何個人資訊的事項作出裁決，並在其認為適當的情況下公布任何此類事件報告。在調查與解決爭議程序，委員會作為合議機構，委員會依法得蒐集履行本法規定職能所需的資料[498]。

(三) 國家隱私委員會調查或處理投訴案件時，發現處理過程中不利於國家安全和公共利益，得中止調查、廢除命令、暫時或永久禁止處理個人資料[499]。

(四) 針對任何隱私相關之請願或政府機關制定命令進行協助或

---

[497] Philippines, Data Privacy Act of 2012, Section 7(a)，Ensure compliance of personal information controllers with the provisions of this Act.

[498] Philippines, Data Privacy Act of 2012, Section 7(b)，Receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report: Provided, That in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the Commission shall act as a collegial body. For this purpose, the Commission may be given access to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act.

[499] Philippines, Data Privacy Act of 2012, Section 7(c)，Issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest;

審查[500]。

(五) 監督其他政府機關針對《資料隱私法》的遵守情況，確保其資訊安全及技術措施達到個人資料保護的最低標準，必要時並建議其採取必要的措施[501]。

(六) 與其他政府機關和非公務機關私營部門協調、制定和實施個人資料保護的計劃和政策[502]。

(七) 定期公布資料保護之法律遵循要點[503]。

(八) 公布個人資料保護與隱私相關之紀錄與彙編，包括各項指標與相關資料[504]。

(九) 向司法部提出起訴和實施《資料隱私法》第 25 至第 29 條規定的處罰[505]。

(十) 審查、核准或否決個人資料持有者自主提出之隱私宣告，該隱私權宣告應遵循《資料隱私法》[506]，該宣告可包括任何個

---

[500] Philippines, Data Privacy Act of 2012, Section 7(d)，Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy;

[501] Philippines, Data Privacy Act of 2012, Section 7(e), "Monitor the compliance of other government agencies or instrumentalities on their security and technical measures and recommend the necessary action in order to meet minimum standards for protection of personal information pursuant to this Act;"

[502] Philippines, Data Privacy Act of 2012, Section 7(f), "Coordinate with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal information in the country;"

[503] Philippines, Data Privacy Act of 2012, Section 7(g), "Publish on a regular basis a guide to all laws relating to data protection;"

[504] Philippines, Data Privacy Act of 2012, Section 7(h), "Publish a compilation of agency system of records and notices, including index and other finding aids;"

[505] Philippines, Data Privacy Act of 2012, Section 7(i), "Recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sections 25 to 29 of this Act".

[506] Philippines, Data Privacy Act of 2012, Section 7(j), "Review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers: Provided, That the privacy codes shall adhere to the underlying data privacy principles embodied in this Act: Provided, further, That such privacy codes may include private dispute resolution mechanisms for complaints against any participating personal information controller. For this purpose, the

人投訴及其他爭議解決機制。委員會應協商相關監管機構制定和管理適用本法規定之標準，並要求相關產業遵循。

(十一) 應公務機關、非公務機關或任何個人的要求，就隱私或個人資料保護事宜提供協助[507]。

(十二) 對中央或地方法令、法規或行政命令關於個人資料或隱私的相關規定進行解釋、發表諮詢意見，並得解釋本法規定和其他隱私相關法規[508]。

(十三) 就國內有關隱私或個人資料保護之法律提出立法、修改之建議[509]。

(十四) 確保與其他國家之隱私主管機構及相關單位進行適當、有效的協調，並參與個人資料、隱私保護的國際組織與活動[510]。

(十五) 與其他國家之個人資料或隱私主管機關談判和簽約，以跨境申請和實施各自的隱私保護相關法令[511]。

Commission shall consult with relevant regulatory agencies in the formulation and administration of privacy codes applying the standards set out in this Act, with respect to the persons, entities, business activities and business sectors that said regulatory bodies are authorized to principally regulate pursuant to the law: Provided, finally. That the Commission may review such privacy codes and require changes thereto for purposes of complying with this Act;"

507 Philippines, Data Privacy Act of 2012, Section 7(k),"Provide assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person".

508 Philippines, Data Privacy Act of 2012, Section 7 (l), "Comment on the implication on data privacy of proposed national or local statutes, regulations or procedures, issue advisory opinions and interpret the provisions of this Act and other data privacy laws;"

509 Philippines, Data Privacy Act of 2012, Section 7(m), "Propose legislation, amendments or modifications to Philippine laws on privacy or data protection as may be necessary;"

510 Philippines, Data Privacy Act of 2012, Section 7(n), "Ensure proper and effective coordination with data privacy regulators in other countries and private accountability agents, participate in international and regional initiatives for data privacy protection;"

511 Philippines, Data Privacy Act of 2012, Section 7(o), "Negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of respective

(十六) 協助本國公司於在國際間遵循各項隱私或個人資料保護法律，以開展業務[512]。

(十七) 其他為促進隱私及個人資料保護之跨境執法，所可能需要的行為[513]。

(十八) 每年向總統與國會報告其執行《資料隱私法》法案之情形，委員會同時應視情況公布隱私保護工作情形，並對社會大眾進行個人資料保護之教育宣導[514]。

---

privacy laws".

[512] Philippines, Data Privacy Act of 2012, Section 7(p)，Assist Philippine companies doing business abroad to respond to foreign privacy or data protection laws and regulations;

[513] Philippines, Data Privacy Act of 2012, Section 7(q), "Generally perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection".

[514] Philippines, Data Privacy Act of 2012, Section 40, "The Commission shall annually report to the President and Congress on its activities in carrying out the provisions of this Act. The Commission shall undertake whatever efforts it may determine to be necessary or appropriate to inform and educate the public of data privacy, data protection and fair information rights and responsibilities".

第十一節　紐西蘭—隱私委員辦公室（OPC）

一、概述

《隱私法（Privacy Act 1993）》是紐西蘭的最主要隱私保障法，於 1993 年 5 月 17 日正式公佈施行，主要規範個人資料保護與隱私保障之相關事宜，該法設置隱私委員並賦予其廣泛的職權以確保個人隱私保護之具體落實，並監督政府以及民間企業持有之個人資料受到適當的保護。該法制定 12 個隱私原則，對各主體如何蒐集、使用、儲存以及披露個人資料做出綱領式的指導。

二、監管對象與主管法規

紐西蘭隱私委員職司《隱私法》的執行實施，依法得監管公務機關及非公務機關，但不具裁罰能力，若經調查認為公務機關有侵犯隱私情形，則將案件提交監察委員審理[515]；認為非公務機關有侵犯隱私情形，則向人權審查法院提起訴訟[516]。

---

[515] New Zealand, Privacy Act 1993,Section 72, "Referral of complaint to Ombudsman (1) Where, on receiving a complaint under this Part, the Commissioner considers that the complaint relates, in whole or in part, to a matter that is more properly within the jurisdiction of an Ombudsman under the Ombudsmen Act 1975 or the Official Information Act 1982 or the Local Government Official Information and Meetings Act 1987, the Commissioner shall forthwith consult with the Chief Ombudsman in order to determine the appropriate means of dealing with the complaint. (2) As soon as practicable after consulting with the Chief Ombudsman under subsection (1), the Commissioner shall determine whether the complaint should be dealt with, in whole or in part, under this Act. (3) If the Commissioner determines that the complaint should be dealt with, in whole or in part, under the Ombudsmen Act 1975 or the Official Information Act 1982 or the Local Government Official Information and Meetings Act 1987, the Commissioner shall forthwith refer the complaint or, as the case requires, the appropriate part of the complaint to the Chief Ombudsman to be dealt with accordingly, and shall notify the complainant of the action that has been taken".

[516] New Zealand, Privacy Act 1993, Section 83, "Aggrieved individual may bring proceedings before Human Rights Review Tribunal. Notwithstanding section 82(2), the aggrieved individual (if any) may himself or herself bring proceedings before the Human Rights Review Tribunal against a person to whom section 82 applies if the aggrieved individual wishes to do so".

三、組織規範

(一) 地位與任免

隱私委員隸屬於司法部[517]，相當於我國之三級機關。隱私委員依法由司法部長任免，任期五年[518][519]。副隱私委員由司法部長建議，隱私委員任命之[520]，免職方式同隱私委員[521]。

(二) 成員

隱私委員應配置 1 個以上之工作人員，負責《隱私法》遵循事宜之宣導、處理依法向隱私委員所提出之請求、配合隱私委員進行調查工作以及其他相關事宜[522]。

---

[517] New Zealand, Privacy Act 1993,Section 2(1)(b), "responsible Minister means the Minister of Justice".

[518] New Zealand, Privacy Act 1993,Section 2(1)(b), "Commissioner means the Privacy Commissioner referred to in section 12 ofthis Act and appointed in accordance with section 28(1)(b) of the Crown Entities Act 2004".

[519] New Zealand, Crown Entities Act 2004, section 28(1)(b), "the Governor-General, on the recommendation of the responsible Minister, in the case of a member of an independent Crown entity".

[520] New Zealand, Privacy Act 1993,Section 15(1), "The Governor-General may, on the recommendation of the Minister, appoint a deputy to the person appointed as Commissioner".

[521] New Zealand, Privacy Act 1993,Section 15(2), Part 2 of the Crown Entities Act 2004, "except section 46, applies to the appointment and removal of a Deputy Commissioner in the same manner as it applies to the appointment and removal of a Commissioner".

[522] New Zealand, Privacy Act 1993.Section23, "Privacy officers It shall be the responsibility of each agency to ensure that there are, within that agency, 1 or more individuals whose responsibilities include—(a) the encouragement of compliance, by the agency, with the information privacy principles:(b) dealing with requests made to the agency pursuant to this Act:(c) working with the Commissioner in relation to investigations conducted pursuant to Part 8 in relation to the agency:(d) otherwise ensuring compliance by the agency with the provisions of this Act".

圖 8 紐西蘭隱私委員領導層組織架構圖

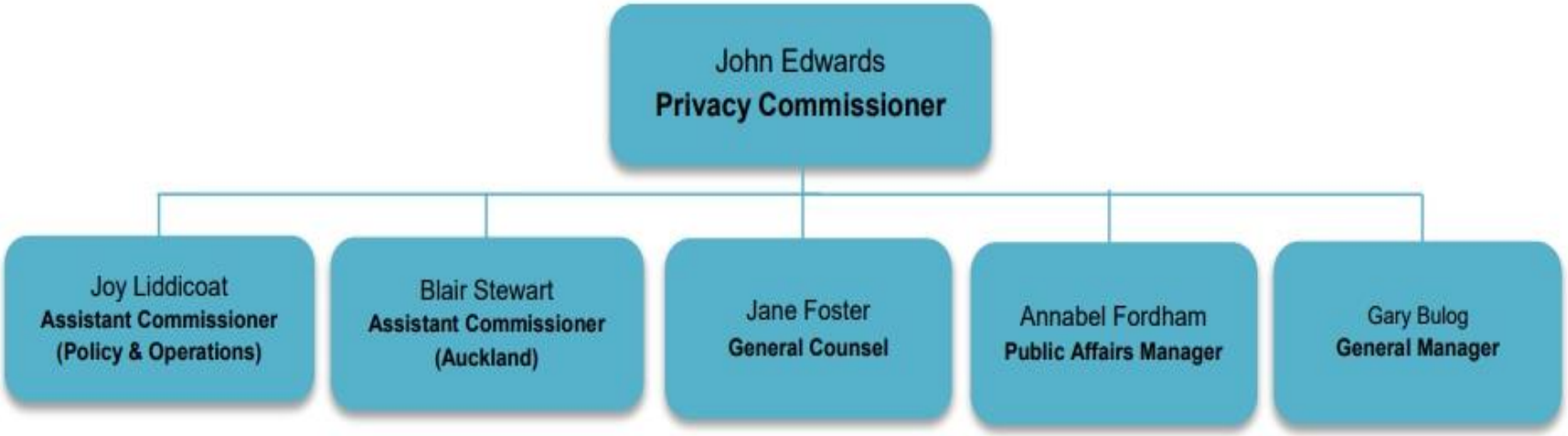


FIGURE 7: Senior Leadership Team

四、法定職務

（一）通過教育和宣傳促進社會大眾認識並接受的隱私及個人資料保護之[523]。

（二）在要求的情況下，對該機構持有之個人資訊進行審核，以確定該個人資料是否根據本法進行維護[524]。

（三）監測唯一標識（unique identifiers）的使用情況，並向內閣總理報告監測結果，並提出包括立法、行政或採取其他行動之必要性或可行性的任何建議以提供個人隱私更完善之保護[525]。

（四）根據《隱私法》第 21 條維護和出版個人資訊目錄[526]。

（五）不定期監督公共隱私權原則的遵守情況，特別是歐洲委員會關於公共機構持有的個人資料向第三方傳達的建議，並向負責部長報告修改這些原則的必要性或可行性[527]。

---

[523] New Zealand, Privacy Act 1993,Section 13(1)(a), “to promote, by education and publicity, an understanding and acceptance of the information privacy principles and of the objects of those principles”.

[524] New Zealand, Privacy Act 1993,Section 13(1)(b), “when requested to do so by an agency, to conduct an audit of personal information maintained by that agency for the purpose of ascertaining whether or not the information is maintained according to the information privacy principles”.

[525] New Zealand, Privacy Act 1993,Section 13(1)(c), “to monitor the use of unique identifiers, and to report to the Prime Minister from time to time on the results of that monitoring, including any recommendation relating to the need for, or desirability of taking, legislative, administrative, or other action to give protection, or better protection, to the privacy of the individual”.

[526] New Zealand, Privacy Act 1993,Section 13(1)(d), “to maintain, and to publish, in accordance with section 21, directories of personal information”.

[527] New Zealand, Privacy Act 1993, Section 13(1) (e), “to monitor compliance with the public register privacy principles, to review those principles from time to time with particular regard to the Council of Europe Recommendations on Communication to Third Parties of Personal Data Held by Public Bodies (Recommendation R (91) 10), and to report to the responsible Minister from time to time on the need for or desirability of amending those principles”.

（六）負責審議公務機關蒐集個人資料或向其他公務機關提供個人資料之法規及修法需求[528]。

（七）為促進個資及隱私保護，應與有關單位合作進行教育活動[529]。

（八）就影響個人或任何類別個資之一切任何活動發表公開聲明[530]。

（九）接受和邀請公眾人士就任何影響個人隱私的事項提出建言[531]。

（十）與其他有關個人隱私之專家或和團體協商和合作[532]。

（十一）對任何與個人隱私保護相關事宜提出建議[533]。

（十二）就有關本法案運作之任何事宜向部長或有關單位機構

---

[528] New Zealand, Privacy Act 1993,Section 13(1) (f), "to examine any proposed legislation that makes provision for—the collection of personal information by any public sector agency; or the disclosure of personal information by one public sector agency to any other public sector agency,—or both; to have particular regard, in the course of that examination, to the matters set out in section 98, in any case where the Commissioner considers that the information might be used for the purposes of an information matching programme; and to report to the responsible Minister the results of that examination".

[529] New Zealand, Privacy Act 1993,Section 13(1) (g), "for the purpose of promoting the protection of individual privacy, to undertake educational programmes on the Commissioner's own behalf or in co-operation with other persons or authorities acting on behalf of the Commissioner".

[530] New Zealand, Privacy Act 1993,Section 13(1) (h), "to make public statements in relation to any matter affecting the privacy of the individual or of any class of individuals".

[531] New Zealand, Privacy Act 1993,Section 13(1) (i), "to receive and invite representations from members of the public on any matter affecting the privacy of the individual".

[532] New Zealand, Privacy Act 1993,Section 13(1) (j), "to consult and co-operate with other persons and bodies concerned with the privacy of the individual".

[533] New Zealand, Privacy Act 1993,Section 13(1) (k), "to make suggestions to any person in relation to any matter that concerns the need for, or the desirability of, action by that person in the interests of the privacy of the individual".

提供諮詢意見[534]。

（十三）在不影響隱私委員職務下，隱私委員應每年提出本法案之年度執行報告[535]。

[534] New Zealand, Privacy Act 1993,Section 13(1) (l), "to provide advice (with or without a request) to a Minister or an agency on any matter relevant to the operation of this Act".

[535] New Zealand, the Crown Entities Act 2004,Section 150, "Obligation to prepare, present, and publish annual report(1)A Crown entity must—(a)as soon as practicable after the end of each financial year, prepare a report on the affairs of the Crown entity; and(b)provide the report to its responsible Minister no later than 15 working days after receiving the audit report provided under section 156.(2)[Repealed](3)A responsible Minister of a Crown entity (or another Minister, if subsection (6) applies) must present the entity's annual report to the House of Representatives within 5 working days after the responsible Minister receives the annual report or, if Parliament is not in session, as soon as possible after the commencement of the next session of Parliament.(4)A Crown entity must publish its annual report as soon as practicable after it has been presented to the House of Representatives, but in any case not later than 10 working days after the annual report is received by the Minister, in a manner consistent with any instructions given under section 174.(5)An entity's annual report may be presented or published in a document that includes any other report or information, whether or not that other report or information relates to the entity, but only if each report or set of information is separately identifiable within that document.(6)A Minister other than the responsible Minister may present an entity's annual report to the House of Representatives if—(a)the report is presented in a document that includes another report or other information; and(b)that other Minister is responsible for presenting that other report or information".

第十二節　澳洲—資訊委員辦公室（OAIC）

一、概述

隨著網際網路、社群媒體與電子通訊軟體的普及，以及各國政府機關與私人企業極力發展各類資訊化服務應用，資訊大量流通為人們帶來了便利與商機，但伴隨而來隱私權侵害的風險也與日俱增，時至今日，隱私權保護趨勢已從過去消極避免當事人隱私權受侵害，轉變為積極防止侵害的發生。澳洲政府為因應此趨勢，於 1988 年末通過了《隱私法（Privacy Act 1988）》，並於 1989 年初施行，又於 2010 年通過《資訊委員法（Australian Information Commissioner Act 2010）》並設置資訊委員負責個人隱私保護等相關議題。

依據《隱私法》以及《資訊委員法》，澳洲政府成立「澳洲資訊委員辦公室[536]」（the Office of the Australian Information Commissioner，以下簡稱 OAIC），專責處理資訊公開與隱私保護事務的整合，並負責政府資訊公開、運用及涉及個人隱私保護等相關議題。

二、監管對象與主管法規

澳洲資訊委員辦公室之監管對象包含公務機關及非公務機關，如調查認有違法行為時，資訊委員可做出行政裁定，並於符合法定程序後由法院進行執行[537]。

---

[536] Australian, Australian Information Commissioner Act 2010, Part2, Sec4, “This Part establishes the Office of the Australian Information Commissioner. The Office of the Australian Information Commissioner consists of the information officers and the staff of the Office.”

[537] Australian, Privacy Act 1988, Part V, Sec55, “Proceedings in the Federal Court or Federal Circuit Court to enforce a determination (1) The following persons may commence proceedings in the

另除《隱私法》外，澳洲資訊委員辦公室亦同時監管《資訊自由法（Freedom of Information Act）》。

三、組織規範

澳洲為聯邦制國家，於中央政府組織中設有「總理內閣部（Department of the Prime Minister and Cabinet）」，該部與其他中央部會之位階相當，主要負責協助總理協調處理跨部會業務。由於隱私保護之議題通常涉及不同部會，故設置澳洲資訊委員辦公室負責協助總理內閣部制定隱私權保護之相關政策，並維持檢查各部會對於隱私權法案之適法性，其位階相當於我國之三級機關。

依據《資訊委員法》設置的澳洲資訊委員辦公室內成員包括資訊委員（Information Commissioner）、資訊公開委員（Freedom of Information Commissioner）及隱私委員（Privacy Commissioner）[538]，而依照《隱私法》所設立之隱私委員辦公室，則成為資訊委

Federal Court or the Federal Circuit Court for an order to enforce a determination: (a) if the determination was made under subsection 52(1)—the complainant; (b) the Commissioner. (2) If the court is satisfied that the person or entity in relation to which the determination applies has engaged in conduct that constitutes an interference with the privacy of an individual, the court may make such orders (including a declaration of right) as it thinks fit. (3) The court may, if it thinks fit, grant an interim injunction pending the determination of the proceedings. (4) The court is not to require a person, as a condition of granting an interim injunction, to give an undertaking as to damages. (5) The court is to deal by way of a hearing de novo with the question whether the person or entity in relation to which the determination applies has engaged in conduct that constitutes an interference with the privacy of an individual. (6) Despite subsection (5), the court may receive any of the following as evidence in proceedings about a determination made by the Commissioner under section 52: (a) a copy of the Commissioner's written reasons for the determination; (b) a copy of any document that was before the Commissioner; (c) a copy of a record (including any tape recording) of any hearing before the Commissioner (including any oral submissions made). (7A) In conducting a hearing and making an order under this section, the court is to have due regard to the objects of this Act. (8) In this section: complainant, in relation to a representative complaint, means any of the class members".

[538] Australian, Australian Information Commissioner Act 2010, Part2, Sec. 6, "Each of the following is an information officer: (a) the Information Commissioner; (b)the Freedom of Information Commissioner; (c)the Privacy Commissioner."

員辦公室的一部分。上述委員均由澳洲總督（the Governor General）任免之[539]，任期最長為五年，負責一切與《資訊委員法》相關之事項，除必須專職擔任外，若有任何有償兼職均需澳洲內閣總理同意[540]，其待遇依據「1973 薪酬法案」，本薪為年薪 310,740 元澳幣（折合新台幣約 748 萬元），加計其他薪酬後年薪不得超過 443,910 元澳幣[541]（折合新台幣約 1,068 萬元）。

依據《資訊委員法》，澳洲資訊委員辦公室係一獨立之法定辦公室，由資訊委員、資訊公開委員以及隱私委員領導，分別就不同業務進行權責之分配[542]。除了上述聯邦組織架構及法令的規範外，在澳洲境內各州及領地內均設有類同於中央資訊委員辦公室之組織，針對各州居民之隱私保護或相關爭議事件之處理。

---

[539] Australian, Australian Information Commissioner Act 2010, Part2, Sec. 14, "Appointment(1) The Australian Information Commissioner is to be appointed by the Governor‐General by written instrument.(2) The Freedom of Information Commissioner is to be appointed by the Governor‐General by written instrument.(3) A person may only be appointed as the Freedom of Information Commissioner if he or she has obtained a degree from a university, or an educational qualification of a similar standing, after studies in the field of law.(4) The Privacy Commissioner is to be appointed by the Governor‐General by written instrument."

[540] Australian, Australian Information Commissioner Act 2010, Part2, Sec. 17, "An information officer must not engage in paid employment outside the duties of his or her office without the Minister's approval".

[541] Australian, Remuneration Tribunal Determination 2016/19: Remuneration and Allowances for Holders of Full-Time Public Office, Sec 2.1.

[542] Australian, Australian Information Commissioner Act 2010, Part2, Sec. 5,"Establishment(1) The Office of the Australian Information Commissioner is established by this section.(2) The Office of the Australian Information Commissioner consists of:(a) the information officers; and(b) the staff mentioned in Part 3.(3) For the purposes of the Public Service Act 1999: (a) the information officers and staff of the Office of the Australian Information Commissioner together constitute a Statutory Agency; and (b) the Information Commissioner is the Head of that Statutory Agency. Note: The Information Commissioner holds an office equivalent to that of a Secretary of a Department (see the definition of Agency Head in section 7 of the Public Service Act 1999)."

圖 9 澳洲資訊委員辦公室組織架構圖

四、法定職務

(一) 隱私權侵害調查

個人可針對可能干擾個人隱私之行為或做法，向澳洲資訊委員辦公室提出投訴或申請調查，資訊委員亦可主動針對干擾個人隱私或違反澳洲隱私原則第 1 條之行為或做法開啟調查程序[543]，調查對象包括，澳洲國民、政府機關及私營企業，如健康服務提供商、信用提供機構及信用報告機構等，有關違反隱私保護之行為，申訴經調查後資訊委員可作成行政裁定，並於符合法定程序後由法院進行執行[544]。

---

[543] Australian, Privacy Act 1988, Part V, Sec. 36A, "In general, this Part deals with complaints and investigations about acts or practices that may be an interference with the privacy of an individual. An individual may complain to the Commissioner about an act or practice that may be an interference with the privacy of the individual. If a complaint is made, the Commissioner is required to investigate the act or practice except in certain circumstances. The Commissioner may also, on his or her own initiative, investigate an act or practice that may be an interference with the privacy of an individual or a breach of Australian Privacy Principle 1.The Commissioner has a range powers relating to the conduct of investigations including powers: (a) to conciliate complaints; and (b) to make preliminary inquiries of any person; and (c) to require a person to give information or documents, or to attend a compulsory conference; and (d) to transfer matters to an alternative complaint body in certain circumstances. After an investigation, the Commissioner may make a determination in relation to the investigation. An entity to which a determination relates must comply with certain declarations included in the determination. Court proceedings may be commenced to enforce a determination."

[544] Australian, Privacy Act 1988, Part V, Sec. 55, "Proceedings in the Federal Court or Federal Circuit Court to enforce a determination(1) The following persons may commence proceedings in the Federal Court or the Federal Circuit Court for an order to enforce a determination: (a) if the determination was made under subsection 52(1)—the complainant; (b) the Commissioner.(2) If the court is satisfied that the person or entity in relation to which the determination applies has engaged in conduct that constitutes an interference with the privacy of an individual, the court may make such orders (including a declaration of right) as it thinks fit.(3) The court may, if it thinks fit, grant an interim injunction pending the determination of the proceedings.(4) The court is not to require a person, as a condition of granting an interim injunction, to give an undertaking as to damages.(5) The court is to deal by way of a hearing de novo with the question whether the person or entity in relation to which the determination applies has engaged in conduct that constitutes an interference with the privacy of an individual.(6) Despite subsection (5), the court may receive any of the following as evidence in proceedings about a determination made by the Commissioner under section 52:(a) a copy of the Commissioner's written reasons for the determination; (b) a copy of any document that was before the Commissioner; (c) a copy of a record (including any tape

(二) 信用資料機構調查權

依《隱私法》之規定，為瞭解信用資料機構在執行個人資料保護相關作業的實際情形，隱私委員得針對信用報告機關（Credit Reporting Bodies[545]）或信用提供者（Credit Providers[546]）所持有之信用報告與信用資料檔進行查核，以調查這些單位在處理相關資料時，是否符合隱私權法或信用資料保護行為準則之規定。

隱私委員亦得受理有關信用報告機構或信貸提供者的投訴，個人可針對信用報告機構或信貸提供者可能違反《隱私法》之行為或做法提出投訴，隱私委員必須調查投訴並對投訴作出決定[547]。亦得檢查信用報告機關與信用提供者之紀錄，確保相關機構並無違法或未經授權而使用個人資料之行為。對於隱私權保護相關查核工作之進行，隱私委員辦公室並訂有隱私查核手冊（Privacy Audit Manual），包含信用資料之查核政策、查核程序，以及查核手續進行時應

---

recording) of any hearing before the Commissioner (including any oral submissions made).(7A) In conducting a hearing and making an order under this section, the court is to have due regard to the objects of this Act.(8) In this section: complainant, in relation to a representative complaint, means any of the class members."

545 Australian, Privacy Act 1988, Part V, Sec. 20, "This Division sets out rules that apply to credit reporting bodies in relation to their handling of the following: (a) credit reporting information; (b) CP derived information; (c) credit reporting information that is de‐identified; (d) a pre‐screening assessment. The rules apply in relation to that kind of information or assessment instead of the Australian Privacy Principles."

546 Australian, Privacy Act 1988, Part V, Sec. 21, "This Division sets out rules that apply to credit providers in relation to their handling of the following: (a) credit information; (b) credit eligibility information; (c) CRB derived information. If a credit provider is an APP entity, the rules apply in relation to that information in addition to, or instead of, any relevant Australian Privacy Principles."

547 Australian, Privacy Act 1988, Part V, Sec. 23, "This Division deals with complaints about credit reporting bodies or credit providers.Individuals may complain to credit reporting bodies or credit providers about acts or practices that may be a breach of certain provisions of this Part or the registered CR code.If a complaint is made, the respondent for the complaint must investigate the complaint and make a decision about the complaint. "

遵守的方針等相關事項。

(三) 稅務檔案號碼管理

稅務檔案號碼是澳洲稅務機關（ATO）發佈用以確認個人、企業等納稅主體的唯一編號，根據《隱私法》，資訊委員有立法規範稅務檔案號碼蒐集、處理和利用方式的權力[548]，其所制定之規定對稅務檔案號碼蒐集者有拘束力[549]。

(四) 隱私保護諮詢委員會

依據《隱私法》第 81 條以下，資訊委員應成立隱私保護諮詢委員會，委員會成員除資訊委員及隱私委員外，其餘委員不超過 8 名均為兼職身分，並由澳洲總督任命之[550]，

---

[548] Australian, Privacy Act 1988, Part V, Sec. 17, "The Commissioner must, by legislative instrument, issue rules concerning the collection, storage, use and security of tax file number information."

[549] Australian, Privacy Act 1988, Part V, Sec. 18, "A file number recipient shall not do an act, or engage in a practice, that breaches a rule issued under section 17."

[550] Australian, Privacy Act 1988, Part V, Sec. 82, "(1) A Privacy Advisory Committee is established.(2) The Advisory Committee shall consist of:(a) the Commissioner; and (aa) the Privacy Commissioner (within the meaning of the Australian Information Commissioner Act 2010); and (b) not more than 8 other members.(3) A member other than the Commissioner and Privacy Commissioner (within the meaning of that Act): (a) shall be appointed by the Governor‐General; and (b) shall be appointed as a part‐time member.(4) An appointed member holds office, subject to this Act, for such period, not exceeding 5 years, as is specified in the instrument of the member's appointment, but is eligible for re‐appointment.(5) The Commissioner shall be convenor of the Committee.(6) The Governor‐General shall so exercise the power of appointment conferred by subsection (3) that a majority of the appointed members are persons who are neither officers nor employees, nor members of the staff of an authority or instrumentality, of the Commonwealth.(7) Of the appointed members:(a) at least one must be a person who has had at least 5 years' experience at a high level in industry or commerce; and(aa) at least one must be a person who has had at least 5 years' experience at a high level in public administration, or the service of a government or an authority of a government; and (ab) at least one must be a person who has had extensive experience in health privacy; and (b) at least one must be a person who has had at least 5 years' experience in the trade union movement; and (c) at least one must be a person who has had extensive experience in information and communication technologies; and (d) at least one must be appointed to represent general community interests, including interests relating to social welfare; and (e) at least one must be a person who has had extensive experience in the promotion of civil liberties.(10) An appointed member holds office on such terms and conditions (if any) in respect of matters not provided for by this Act as are determined, in writing, by the Governor‐General.(11) The performance of a function of the Advisory Committee is not affected because of a vacancy or vacancies in the membership of the Advisory Committee."

其主要任務在於主動或依資訊委員之指示就相關事項提出建議或報告，以及針對隱私保護議題進行社區教育或社區諮詢。

(五) 醫療研究指導準則之核准權

依據《隱私法》，個人醫療資訊之蒐集、處理與利用受到嚴密規範，以保障個人隱私，惟醫療研究在許多狀況下實難取得病患同意《隱私法》為了醫療研究目的，賦予資訊委員對國家健康醫療研究理事會所制定之研究指導準則擁有核准之權利，以兼顧隱私保護與醫療研究需要[551]。

[551] Australian, Privacy Act 1988, Part IX, Sec. 95,"(1) The CEO of the National Health and Medical Research Council may, with the approval of the Commissioner, issue guidelines for the protection of privacy by agencies in the conduct of medical research.(2) The Commissioner shall not approve the issue of guidelines unless he or she is satisfied that the public interest in the promotion of research of the kind to which the guidelines relate outweighs to a substantial degree the public interest in maintaining adherence to the Australian Privacy Principles.(3) Guidelines shall be issued by being published in the Gazette.(4) Where: (a) but for this subsection, an act done by an agency would breach an Australian Privacy Principle; and (b) the act is done in the course of medical research and in accordance with guidelines under subsection (1);the act shall be regarded as not breaching that Australian Privacy Principle."

第十三節　個資與隱私保護委員國際研討會（ICDPPC）

於 2017 年舉辦第 39 屆的「個資與隱私保護委員國際研討會（International Conference of Data Protection and Privacy Commissioners，ICDPPC）」係一由世界各國個資與隱私保護主管機關代表參與的國際會議，乃目前全球最重要的個資與隱私保護監理法制會議。

該國際會議之議程區分為「公開議程」及「非公開議程」，其中「非公開議程」僅會員或觀察員得參與。

一、會員及資格

依 ICDPPC 公布之《個資與隱私保護委員國際研討會規則與程序（International Conference of Data Protection and Privacy Commissioners RULES AND PROCEDURES）》[552]，符合下列條件之主管機關始得申請成為會員：

（一）法定公務機關

該主管機關應為依所屬國家或國際組職的法規適當設置之公務機關[553]。

（二）法定任務

該主管機關的法定任務之一應為監督個資或隱私保

---

[552] https://icdppc.org/wp-content/uploads/2015/02/Rules-and-Procedures.pdf，最後到訪為 106 年 9 月 18 日。

[553] 《International Conference of Data Protection and Privacy Commissioners RULES AND PROCEDURES》, ICDPPC, 2017, Section5.1(a), " A public entity, created by an appropriate legal instrument based upon legal traditions of the country or international organisation which it belongs to".

護法律的落實[554]。

（三）法律合規

該主管機關監管之法律內容應與個資或隱私保護的國際原則相符[555]。

（四）法定職權

該主管機關應有適當的法定職權以行使其任務[556]。

（五）自主獨立

該主管機關應具備適當的自主性及獨立性[557]。

截至本研究報告交付日止，ICDPPC 共有下列國家的個資保護主管機關加入成為會員：安道爾、阿根廷、**澳洲**（聯邦隱私委員、新南威爾斯隱私委員、北境資訊委員、維多利亞隱私委員即隱私及個資保護委員）、**加拿大**（隱私委員、亞伯達資訊及隱私委員、英屬哥倫比亞資訊及隱私委員、曼尼托巴監察使、新布倫瑞克監察使、紐芬蘭與拉布拉多資訊及隱私委員辦公室、西北區資訊及隱私委員、新斯科舍資訊自由及隱私保護審查辦公室、努納福特資訊及隱私委員、安大略資訊及隱私委員、魁北克資訊近

554 《International Conference of Data Protection and Privacy Commissioners RULES AND PROCEDURES》, ICDPPC, 2017, Section5.1(b), “Has the supervision of the implementation of the legislation on the protection of personal data or privacy as one of its principal regulatory mandates”.

555 《International Conference of Data Protection and Privacy Commissioners RULES AND PROCEDURES》, ICDPPC, 2017, Section5.1(c), “The legislation under which it operates is compatible with the principal international instruments dealing with data protection or privacy”.

556 《International Conference of Data Protection and Privacy Commissioners RULES AND PROCEDURES》, ICDPPC, 2017, Section5.1(d), “Has an appropriate range of legal powers to perform its functions”.

557 《International Conference of Data Protection and Privacy Commissioners RULES AND PROCEDURES》, ICDPPC, 2017, Section5.1(e), “Has appropriate autonomy and independence”.

用委員會、薩斯喀徹溫資訊及隱私委員）、歐盟（海關資訊系統聯合監督機關、歐盟個資保護監督機關 EDPS、歐洲司法組織聯合監督機構 Joint Supervisory Body of Eurojust）、德國、**香港**、根西、曼島、以色列、**日本**、澤西、墨西哥、**紐西蘭**、**菲律賓**、**南韓**（資料安全局 Korea Information Security Agency、個資保護委員會）、瑞士、**英國**、美國 FTC、烏拉圭。

二、觀察員及資格

除申請加入成為會員外，不符合會員資格者如具備下列條件，亦可申請成為 ICDPPC 的觀察員：

（一）不具備會員條件，但參與個資保護執行的公務機關[558]

例如加拿大國際工業安全理事會、南韓內政部、美國國土安全隱私辦公室、美國聯邦通訊委員會。

（二）與個資或隱私保護活動相關的國際組織[559]

例如歐洲議會、歐盟執委會、紅十字會。

（三）其他基於互惠原則授予 ICDPPC 觀察員資格的組織[560]

例如 APEC 電子商務指導小組。

---

[558] 《International Conference of Data Protection and Privacy Commissioners RULES AND PROCEDURES》, ICDPPC, 2017, Section5.3(a), “Public entities that do not meet [the criteria provided for in article 5.1], but are involved in dealing with the protection of personal data and/or privacy”.

[559] 《International Conference of Data Protection and Privacy Commissioners RULES AND PROCEDURES》, ICDPPC, 2017, Section5.3(b), “International organisations whose activity is related to the protection of personal data or privacy”.

[560] 《International Conference of Data Protection and Privacy Commissioners RULES AND PROCEDURES》, ICDPPC, 2017, Section5.3(c), “Any other organisation that has granted Observer status to the Conference, under the principle of reciprocity”.

除前述觀察員外，在 2017 年的 ICDPPC 研討會中，南韓通訊委員會（KCC）、**新加坡**個資保護委員會及**馬來西亞**個資保護署均是本屆觀察員。

由上研究發現可知，本研究之研究對象除澳門個人資料保護辦公室外，均已成為 ICDPPC 的會員或觀察員，可每年定期與全球個資與隱私保護主管機關進行國際交流與合作接觸，值得我國借鏡。

第十四節　APEC 跨境隱私保護規則體系（CBPRs）

一、CBPRs 簡介

亞洲太平洋經濟合作會議（APEC）為促進經濟區內個人資料的自由流動，避免各會員經濟體的隱私保護規範落差形成個資跨境流通的阻礙，並同時保障個資當事人權利，特制定「跨境隱私保護規則體系（Cross Border Privacy Rules System, CBPRs）」供會員經濟體加入。

CBPRs 提供一套「隱私框架（APEC Privacy Framework）」供會員經濟體內的民間企業遵循落實，並申請取得驗證，以此提升彼此對個資保護的信任。

二、加入 CBPRs 程序[561]

會員經濟體需先由至少一個「隱私保護執法機關 Privacy Enforcement Authorities（PEA）」參與「跨境隱私保護執法協議（Cross-border Privacy Enforcement Arrangement, CPEA）」，該協議係為建置 APEC 區域內的隱私及個資保護法律執行之區域性合作框架。

其次，會員經濟體應向 APEC 電子商務指導小組（APEC Electronic Commerce Steering Group, ECSG）、資料隱私小組（Data Privacy Subgroup, DPS）及聯合監督工作小組（APEC CBPR system Joint Oversight Panel , JOP）提出加入 CBPR 的申請，申請內容包含：

---

561 見 http://www.cbprs.org/Government/EconomiesRequirements.aspx，最後到訪日為 107 年 1 月 4 日。

（一）確認經濟體內已有一個隱私保護執法機關加入跨境隱私保護執法協議。

（二）確認經濟體有意指定至少一個已經或將經 APEC CBPRs 認許之「當責機構（Accountability Agent , AA）」。

（三）具體描述「經濟體管轄區內之當責機構適用的相關法律、法規及行政措施」、「執行相關法律、法規及行政措施之一個或數個主管機關」及「相關法律、法規及行政措施之執行方式」。

同時，經濟體也應填具相關文件，詳細說明與 CBPRs 關於個資保護之要求具備一致性之相關法律、法規與行政措施，並描述相關法律、法規與行政措施如何在經濟體管轄區內執行。

最後，聯合監督工作小組將於審查後發布結果報告，通過審查之會員經濟體即於報告發布日正式加入 CPBRs。

三、申請成為當責機構 AA 程序[562]

如前所述，加入 CBPRs 的經濟體應指定至少一個組織作為當責機構，其功能在於驗證申請加入 CBPRs 的企業是否符合「隱私框架（APEC Privacy Framework）」的規範，並於可能的範圍內協調解決企業、消費者及政府間的爭端。

組織（不限公務機關或非公務關）欲申請成為當責機構，必須符合 APEC 規定應備之條件（Criteria）[563]，並填妥、備齊文

---

562 見 http://www.cbprs.org/Agents/NewAgentProcess.aspx，最後到訪日為 107 年 1 月 4 日。

563 見 https://cbprs.blob.core.windows.net/files/Accountability%20Agent%20Recognition%20Criteria.pdf，最後到訪日為 107 年 1 月 4 日。

件向主管機關提出申請，經初步審查後，主管機關將向 APEC 電子商務指導小組、資料隱私小組及聯合監督工作小組提交該申請文件。

聯合監督工作小組將審查申請內容並向電子商務指導小組提出意見，並將交付所有 APEC 會員經濟體徵詢意見。在聯合監督工作小組發布意見報告前，小組或 APEC 會員經濟體均有可能要求申請之組織補充證明文件或提出說明。

最後，如聯合監督工作小組審查通過組織之申請，仍將給予 APEC 會員經濟體一段期間表達反對之意，如無反對意見，則該組織即在期間屆滿後成為當責機構。

四、隱私保護執法機關

CBPRs 對於各會員經濟體之「隱私保護執法機關」的定義規範於《跨境隱私保護執法合作協議（APEC COOPERATION ARRANGEMENT FOR CROSS-BORDER PRIVACY ENFORCEMENT）》第 4.1 條中，即指該經濟體內負責實施隱私保護法律且得行使調查權或執行執法程序之公務機關[564]。

五、已加入 CPEA 及 CBPRs 之經濟體及隱私保護執法機關

截至本研究報告交付日止，目前共有來自 10 個會員經濟體（澳洲、加拿大、香港、日本、南韓、紐西蘭、美國、墨西哥、新加坡、菲律賓）的 11 個隱私保護執法機關加入該跨境隱私保

564 《APEC COOPERATION ARRANGEMENT FOR CROSS-BORDER PRIVACY ENFORCEMENT》, 4.1, “Privacy Enforcement Authority’ means any public body that is responsible for enforcing Privacy Law, and that has powers to conduct investigations or pursue enforcement proceedings”.

護執法協議，分別為：**澳洲**資訊委員辦公室（OAIC）、**紐西蘭**隱私委員辦公室（OPC）、美國聯邦貿易委員會（FTC）、**香港**個人資料私隱專員公署（PCPD）、**加拿大**隱私委員辦公室（OPC）、南韓內政部（MOI）、南韓通訊委員會（KCC）、墨西哥聯邦資訊查閱及個資保護局（Federal Institute for Access to Information and Data Protection of Mexico）、**新加坡**個資保護委員會（PDPC）、**日本**個人資訊保護委員會[565]、**菲律賓**國家隱私委員會（NPC）[566]，其中美國、墨西哥、日本、加拿大及南韓已加入跨境隱私保護規則體系，新加坡也在申請加入之列，菲律賓亦有意提出申請。

[565] 見 https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx，最後到訪日為 107 年 1 月 4 日。

[566] 見 http://www.philstar.com/business/2017/12/07/1765918/philippines-joins-cross-border-privacy-enforcement-arrangement，最後到訪日為 107 年 1 月 4 日。

第十五節　研究發現整理

一、研究國家均設有獨立個資保護專責機關

由本研究所選各國法例比較觀察可知，有個資或隱私保護專法的國家均已設置個資或隱私保護專責「機關」，即「得以自己名義決定並對外表示行政主體意思，具有單獨法定地位之組織」，性質應同於我國《中央行政機關組織基準法》第 3 條第 1 款定義的「機關」[567]及《行政程序法》第 2 條第 2 項定義的「行政機關」[568]，具有組織法規並以具備獨立之人員編制及預算為原則。包含日本亦於 2016 年成立個人資訊保護委員會，專門負責監管日本個人情報保護法的落實（見下表）。

又各「專責」機關並非均「僅主管個資或隱私保護專法」，尚可主管其他與個資或隱私保護相關法律（例如資訊自由法、電子通訊法等，見下述）。

表 1 各國個資與隱私保護專責機關彙整表

國家	專責機關與成立年度 首長任免及機關地位	相當或類似 我國層級
英國	資訊委員辦公室（Information Commissioner ‘s Office, ICO）,1984（原負責個資保護登記 Data	性質類似我國行政法人，例如國家災害防救中心，但具有執行公權力

[567] 中央行政機關組織基準法，第 3 條第 1 款，「本法用詞定義如下：一、機關：就法定事務，有決定並表示國家意思於外部，而依組織法律或命令（以下簡稱組織法規）設立，行使公權力之組織」。

[568] 行政程序法，第 2 條第 2 項，「本法所稱行政機關，係指代表國家、地方自治團體或其他行政主體表示意思，從事公共事務，具有單獨法定地位之組織」。

	Protection Registrar） 資訊委員由英國女王任命，向國會負責。資訊委員辦公室為英國「非部會公機關 non-departmental public body 」之半官方機構，行政法人	特性，異於我國行政法人法之規定
加拿大	隱私委員辦公室（Office of the Privacy Commissioner of Canada, OPC）,1983 隱私委員由加拿大總督經國會同意後任命，對國會負責	無
香港	個人資料私隱專員公署,1996 私隱專員由香港行政長官任命,公署為非政府部門的半官方公營機構	性質類似我國行政法人，例如國家災害防救中心，但具有執行公權力特性，異於我國行政法人法之規定
澳門	個人資料保護辦公室,2007 辦公室主任由行政長官任命，辦公室受行政長官監督（同新聞局、政府發言人辦公室等）。	總統府、國安會
日本	個人情報保護委員会,2016	行政院下的二級

	委員長由首相經國會同意後任命，屬內閣府外局之委員會，由首相及內閣總理大臣管轄	機關（署）
南韓	個人資訊保護委員會（Personal Information Protection Commission，PIPC），2011 委員由總統任命，向總統負責。	總統府、國安會
新加坡	個人資料保護委員會（Personal Data Protection Commission，PDPC），2013 委員會於 2016 年併入新加坡資訊通信媒體發展局，由該局兼管個資保護業務，該局隸屬新加坡通訊及新聞部，由部長任命人事	行政院部會下四級機關
菲律賓	國家隱私委員會（National Privacy Commission） 隱私保護委員由總統任命，委員會隸屬於菲律賓國家資通訊技術部	行政院部會下三級機關（署、局）
馬來西亞	個人資料保護署（Department of Personal Data Protection），2011 個資保護委員由馬來西亞通訊與多	行政院部會下三級機關（署、局）

	媒體部部長任命，隸屬於該部	

二、歐盟及國際組織對個資保護專責機關的要求

本研究之研究對象歐盟、ICDPPC 及 APEC CBPRs 對於會（成）員的個資保護機關要求之條件不盡相同，整理如下：

（一）歐盟

作為全球個資與隱私保護指標的歐盟，特重個資保護機關的「獨立性」及「任務與職權」(詳見本研究報告第二章第一節)，就「**獨立性**」而言，可區分為：

1、組織獨立

依《個資保護規則》第 51 條第 1 項規定，各會員國應設立一個以上的獨立監督機關以負責監管《個資保護規則》的落實。

不過依前述歐洲法院判決之見，監督機關即便於組織架構上隸屬於上級行政機關，只要有其他措施能無損其「完全之獨立性」，即監督機關「不可有『事前遵循』上級機關意旨之可能」且「其決定須客觀、公正，不能有偏頗之虞」，並能「確保不直接或間接受來自外部的任何影響」，便不致牴觸法律所要求的組織獨立性。

2、人事獨立

依《個資保護規則》第 52 條第 4 項規定，各會

員國應確保監督機關享有機關的人事決定權；依《個資保護規則》第 52 條第 3 項規定，無論有無酬勞，監督機關成員應避免任何與其任務相悖之行為，並不得於在職時擔任任何與其任務相悖之職位；依《個資保護規則》第 53 條第 3 項規定，監督機關成員應依會員國法律規定，於其任期屆滿、辭職或強制退休時終止其任務；依《個資保護規則》第 53 條第 4 項規定，監督機關成員僅在發生嚴重不當行為或不再具備其任務所需條件時始能被解雇。

又依前述歐洲法院對匈牙利的判決 Case C-288/12 之見，即便會員國經由立法程序設立新監督機關取代原監督機關，如因此使原監督機關首長提前終止其任期，亦視為係侵害人事獨立性的行為。

相對而言，烏拉圭的個資保護監督機關於 2009 年政權移轉後並無任何變動，即是讓歐盟認定該機關具備足夠人事獨立性的證明。

3、功能獨立

依《個資保護規則》第 52 條第 1 項規定，各監督機關在執行《個資保護規則》所定任務及行使職權時，應享有完全之獨立性；第 52 條第 2 項規定，監督機關成員在依《個資保護規則》執行其任務及行使職權時，應保有不受外來直接或間接影響的自主性，並不得接受或尋求任何人的指示。

此外，依前述歐盟執委會審查境外國家的個資保護適足性之例，「監督機關的決定（處分）僅能由司法審查推翻」亦可作為該監督機關具備功能上獨立性的佐證。

但須留意依前述歐洲法院判決的認定，法律授予會員國個資保護監督機關依法獨立行使職權的功能上獨立性，並不代表該監督機關在組織、人事及財務上均具備完全之獨立性而可不受直接或間接來自外部的任何影響。

4、財務獨立

依《個資保護規則》第 52 條第 4 項規定，各會員國應確保提供各監督機關必要的人力、技術、經費、場所、設施，以供其有效執行法定職務及行使職權；依《個資保護規則》第 52 條第 6 項規定，各會員國應確保各監督機關的財務控管不致影響其獨立性，並享有可包含於整體國家預算中的專屬公務年度預算。

不過，歐洲法院在前述對奧地利的判決 Case C-614/10 中指出，即便個資保護監督機關不具獨立之預算亦不必然影響其獨立性，但監督機關的必要資源之來源不得使其在執行任務時無法具備完全之獨立性，因此若監督機關執行任務所需之人力、設施、場所等資源均來自隸屬的行政機關時，即有可能影響其獨立性。

又在前述歐盟執委會審查境外國家以色列的個資保護適足性時，一併考量以色列個資保護監督機關依法成立基金，將收取之資料庫註冊費納入，並歸該機關使用以執行任務，此亦強化其財務上的獨立性。

再就「**任務與職權**」而言，國際實務上即有個資與隱私保護法律工作者（Centre for Information Policy Leadership at Hunton & Williams LLP）將歐盟《個資保護規則》賦予監管機關之任務與職權區分為「指導（Leader）」、「核准（Authoriser）」、「執法（Police Officer）」及「申訴處理（Complaint-Handler）」等 4 大類，本研究翻譯引用如下[569]：

表 2 歐盟個資保護監督機關任務與職權分類表

歐盟個資保護監督機關任務／職權	GDPR 條文
指導（Leader）	
提升公民對於處理個資的風險、規則、安全維護、當事人權利的意識。	57.1(b)
提升資料控制者與受託者對《個資保護規則》所定義務之認知。	57.1(d)
對國會、政府等機關提出建議。	57.1(c)
提供當事人行使權利之資訊。	57.1(e)

[569] 《Regulating for Results: Strategies and Priorities for Leadership and Engagement discussion paper》, Annex A – DPA Functions Under GDPR, Centre for Information Policy Leadership ("CIPL") at Hunton & Williams LLP, 2017.

監督《個資保護規則》之適用。	57.1(a)
掌握相關資通訊及商業實務的發展。	57.1(i)
答覆資料控制者之諮詢。	57.1(l)
鼓勵並促進實務指引、驗證機制及相關標章。	57.1(m)-(q)
核准（Authoriser）	
核准基於公共利益的高風險個資處理行為。	58.3(c)
核准跨境傳輸個資的契約條款。	58.3(h)
核准跨境傳輸個資的行政協議。	58.3(i)
核准約束性企業規則。	58.3(j)
認許指引、驗證機制及相關標章。	42,43,57,58,64 等
執法（Police Officer）	
監督並實施《個資保護規則》。	57.1(a)
對《個資保護規則》的適用執行調查。	57.1(h)
命資料控制者及受託者提交資訊。	58.1(a)&(e)
訪查資料控制者或受託者的處所、設備及工具。	58.1(f)
發布警示或告誡處分。	58.2(a)-(b)
命令資料控制者或受託者遵循法規。	58.2(c)-(e)
限制或禁止處理個資。	58.2(f)
要求更正、刪除個資等行為。	58.2(g)
科處罰鍰。	58.2(i)
禁止跨境傳輸個人資料。	58.2(j)
申訴處理（Complaint-Handler）	
受理並調查申訴。	57.1(f)

值得注意的是，歐盟在判斷境外國家或地區是否具

備「個資保護適足性」時，考量「監管機關能力」的參考依據包含「**該監管機關是否主辦或參加前述 ICDPPC 及 APEC CBPRs 等國際組織**」，例如在 2009 年對以色列法律、資訊與科技管理局進行審查時，該局將於 2010 年舉辦第 32 屆 ICDPPC 一事即為歐盟認定該監管機關具備足夠個資保護執行能力之依據[570]；又於 2011 年審查紐西蘭個資隱私委員辦公室時，該辦公室係 ICDPPC 的會員且加入 APEC 跨境隱私執法協議一事亦成為歐盟判斷該監督機關個資保護能力的參考[571]。

（二）ICDPPC

如本研究報告第二章第十三節所述，國際個資與隱私保護委員研討會 ICDPPC 對會員的資格要求為「該會員須為法定公務機關」、「該會員之法定任務應包含監管個資或隱私保護法律」、「該會員監管之個資或隱私保護法律內容須與國際原則相符」、「該會員須有適當的法定職權以行使任務」及「該機關須有自主性及獨立性」。

以前述條件檢視我國現況，作為個資法主管機關的法務部是否因「僅對所轄事業有執行調查或裁罰之權」而不符合 ICDPPC 要求「會員須有適當的法定職權以行

570 《Opinion 6/2009 on the level of protection of personal data in Israel》, WP165, 2009, p15, "…and the fact that ILITA has been designated to organize the 32nd International Conference on Privacy and Personal Data Protection, which is scheduled to be held in Jerusalem in October 2010, reinforce the efforts made by the State of Israel to guarantee the existence of a personal data protection authority and to adequately safeguard this right".

571 《Opinion 11/2011 on the level of protection of personal data in New Zealand》, WP182, 2011, p13, "In addition the Office of the Privacy Commissioner has been accredited to the International Conference of Data Protection and Privacy Commissioners; has been approved as a participant of the APEC Cross-border Privacy Enforcement Arrangement".

使任務」的條件，值得觀察；至其他中央目的事業主管機關例如 NCC、公平交易委員會等，亦可能因「法定任務不包含監管個資法」或「僅對所轄事業有執行調查或裁罰之權」等因素而無法申請加入會員。

惟即便無法成為會員，申請成為觀察員應也是我國促進個資與隱私保護國際交流的可行作為，南韓內政部及通訊委員會即為借鏡。

（三）APEC CBPRs

如本研究報告第二章第十四節所述，APEC 跨境隱私保護規則體系對會員經濟體的隱私保護執法機關之要求為「須為公務機關」、「其任務包含實施隱私保護法律」及「須有行使調查或執行執法程序之權利」。

對應上述條件，我國如欲申請加入 CBPRs，似可以例如法務部、經濟部、內政部、金管會、國家通訊傳播委員會、公平交易委員會等中央目的事業主管機關作為參與「跨境隱私保護執法協議」的隱私保護執法機關，其中經濟部已於 2017 年表達加入意願[572]。

三、各國個資保護專責機關監管對象與主管法規

（一）監管對象

由前述研究發現可知，研究國家的個資或隱私保護專

[572] 《辦理 APEC 跨境隱私保護研討會　經部：目標加入 CBPR 體系》，見 http://www.economic-news.tw/2017/10/APEC-CBPR.html，最後到訪為 106 年 1 月 16 日。

責機關之監管對象為：

1、包含公務機關及非公務機關

（1）英國、香港、澳門：均有處罰權。

（2）加拿大：調查後如認有違法情形，得向法院聲請進入司法程序。

（3）菲律賓：無處罰權，僅得向法務部建議處罰。

（4）紐西蘭：無裁罰權，針對公務機關之違法情形提交監察委員；針對非公務機關之違法情形責向人權審查法院提起司法程序。

（5）澳洲：調查後如認有違法情形可作出裁定，在符合法定程序後由法院執行。

2、僅公務機關

南韓：雖無直接裁罰公務機關之權限，惟因其直接隸屬於國家元首，超乎各部會之上，直接向總統負責，故能有效、充分透過審議、決議各公務機關之個人資料保護政策以監督各公務機關個資保護事務之推動。

3、僅非公務機關

（1）日本

（2）馬來西亞

（3）新加坡（但能對公務機關提出建議）

除此之外，ICDPPC 於 2017 年公布的調查報告中指出[573]，就監管對象部分，回覆調查的 86 個個資保護專責機關中：

1、有 73 個同時監管公務機關與非公務機關；

2、12 個僅監管公務機關；

3、另有 1 個僅監管非公務機關。

（二）主管法規

另由前述研究發現可知，英國及澳洲的個資或隱私保護專責機關除主管個資或隱私保護法律外，尚監管其他相關法律，例如資訊自由法、隱私與電子通訊規則等。

又 ICDPPC 於前述報告中亦就此部分提出調查，回覆調查的 87 個個資保護專責機關中：

1、有 38 個同時主管「資訊近用（Information Access）」或「資訊自由（Freedom of Information）」法規；

2、28 個同時主管「濫發電子通訊（Unsolicited Electronic Communications）」或「垃圾郵件（Spam）」法規；

3、28 個同時主管「健康資訊（Health Information）」法規；

4、19 個同時主管「電子通訊（Telecommunications）」法規；

[573] 《Counting on Commissioners：High level results of the ICDPPC Census 2017》 ICDPPC, 2017, p14。

5、14 個同時主管「網路安全（Cyber Security）」法規；

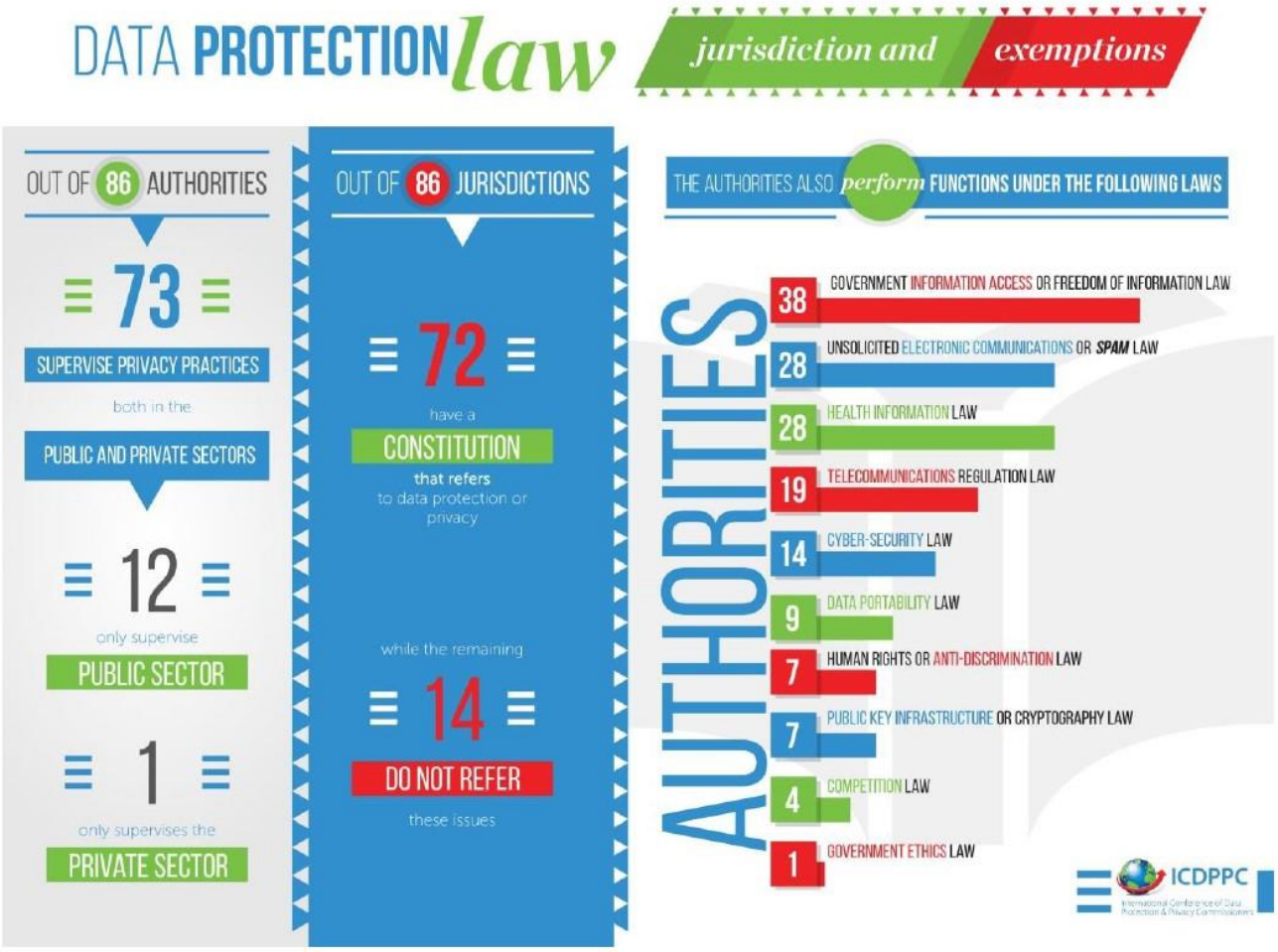
6、9 個主管「資料攜取（Data Portability）」法規；

7、7 個主管「人權（Human Rights）」或「反歧視（Anti-Discrimination）」法規；

8、7 個同時主管「大眾關鍵基礎設施（Public Key Infrastructure）」或「密碼（Cryptography）」法規；

9、4 個同時主管「競爭（Competition）」法；1 個同時主管「政府倫理（Government Ethics）」法規。

圖 10 ICDPPC 個資保護專責機關監管對象及主管法規調查報告



四、法定職務差異

我國個資法賦予中央目的事業主管機關的法定職權或任務與各國規範存有落差，恐使本法的監管與實施效能有所不足。其中重要差異對照整理如下：

表 3 各國個資保護專責機關重要職務對照表

法定職權	台灣（法務部）	台灣（主管機關）	歐盟	英國	加拿大	香港	澳門	日本	南韓	新加坡	馬來西亞	菲律賓	紐西蘭	澳洲
法律解釋	O		O		O	O			O			O		
受理申訴		O	O	O	O	O	O				O	O		O
於調查時要求提出文物		O	O	O	O	O	O	O	O	O	O	O		O
於調查時扣留、複製文物		O		O	O						O			
為調查而進入處所		O		O	O	O		O		O	O			
作出執行通知(限期改善之行政處分)		O	O	O		O	O	O			O	O		

稽核或評估個資法遵、管理、安全		O	O	O	O	O	O					O	
限制或許可跨境傳輸		O	O	O		O	O	O		O	O	O	
行政處罰裁罰能力		O	O	O			O	O		O		O	O
實務守則			O	O	O	O	O	O		O	O	O		
法律或實務研究			O		O	O		O		O	O			
公眾教育			O		O			O		O	O	O	O	O

*以上圈選項目為該機關之組織法規規定的法定職務，未圈選者仍可能依該國其他法規而屬法定職務。

第十六節　vTaiwan 線上意見

研究團隊為協助委託機關徵集公眾意見，於 2017 年將本研究期中報告初步發現與建議製作成簡報上傳至 vTaiwan 平台，於 2017 年 11 月 8 日至 12 月 31 日間就「我國成立個資與隱私保護專責機關」一事徵集公眾意見（**詳見附件**），約略整理如下：

一、專責機關之需求及必要性

就我國成立個資與隱私保護專責機關之「需求及必要性」，155 位填問卷者中有 154 人回答本題，其中 92%認為我國應成立個資與隱私保護專責機關，並有 91%認為該機關應具備獨立性，58%認為應為行政機關。

二、專責機關監管對象

就個資與隱私保護專責機關之「監管對象」，155 位填問卷者中有 83 人回答本題，其中 94%認為除監督民間企業外，應監督公務機關。

三、專責機關之獨立性

就個資與隱私保護專責機關應具備的「獨立性」要素，155 位填問卷者中有 10 人回答本題，其中有認為獨立性要素應指不得兼任利益衝突之職位、獨立組織法規、人事獨立、不受他人指示、有作成行政處分的能力、有獨立預算等。

四、專責機關之法律層級

就個資與隱私保護專責機關的「法律層級」，155 位填問卷者中有 153 人回答本題，其中有 62%認為應成立二級獨立機關，

27%認為應成立三級獨立機關，19%認為應成立二級行政機關，9%認為應成立三級行政機關。

五、專責機關的委員組成

就個資與隱私保護專責機關如為委員制的合議機關，其「民間委員是否應過半數」，155 位填問卷者中有 105 人回答本題，其中有 78%認為專責機關之委員應該過半數為民間委員。

第十七節　研究建議（代本章結論）

一、成立專責機關應具備之要件

綜上研究發現與 vTaiwan 線上徵詢之公眾意見，我國如成立個資保護專責機關，除可統一解釋個資法並於個案中認定事實涵攝之外，亦可發揮「事前指導」功能，協助並輔導我國公務機關與非公務機關妥善遵循與因應法律規範，並能有一致性的標準執行行政檢查與行政處罰。

因歐盟將於 2018 年 5 月生效的 GDPR 之法律適用範圍具備全球性，為使適用 GDPR 的我國企業能在政府的法律框架之下不致遭遇重大阻礙，本研究認為我國如欲成立個資保護專責機關，應以歐盟 GDPR 之標準設立個資保護專責機關，作為政府協助企業發展的第一步[574]，爰以下參考相關外國立法例，提出成立專責機關應具備之要件：

(一) 個資保護應有專責性

本研究認為，基於下列理由，成立個資保護機關應具備專責性：

1、 統一監管個資法

（1）統一解釋法律與認定事實

現行個資法雖以法務部為有權解釋機關，但因涉及個案事實認定，原應由中央目的事業主管

[574] 雖然在政治現實考量下，即便依歐盟標準成立個資保護專責機關，我國恐仍無法獲歐盟認定為具備個資保護適足性之國家，但對須適用 GDPR 的台灣企業而言，我國如有個資保護專責機關，即可發揮協調、法遵等功能，俾利企業合法處理與國際傳輸歐盟自然人之個資。

機關綜合各種情況，本於權責予以審認，惟恐有類似事件，發生不同事實認定之虞，因此，由專責機關統一解釋法律與認定事實，有其必要。

（2）統一執行行政裁罰

除統一解釋法律之外，亦應由單一機關統一執行行政裁罰，避免類似違法卻有寬嚴不一處罰基準的差別對待。

（3）統一監管標準

由單一機關監管個資法，亦能避免各中央目的事業主管機關對所轄事業監督強度不一的情況。

2、促進個資保護的專業化

（1）法律監管具備高度專業性

個資法的監管須有法律、管理、技術及稽核等高度專業，如將本法的調查權及裁罰權歸由各中央目的事業主管機關負責，個別主管機關的執法能量恐嫌不足。

（2）專屬財務與足夠人力有利推動法律執行

承上，執行個資法所需的高度專業性亦體現於主管機關的財務與人力資源面向，如以專責機關負責本法的執行、監管，將有足夠資源落實個人資料保護。

（3）個資保護的事前遵循與教育訓練

個人資料保護在新興網路科技的發展下益發重要且其威脅來源更為多元，個資蒐集者實有賴主管機關的實務指引以茲事前遵循，避免觸法；且民眾亦須主管機關以各種形式的認知與教育訓練來喚起個資保護的意識。

3、 符合國際潮流並強化個資保護的國際合作

（1）設立個資保護專責機關為國際趨勢

如本研究所示，不僅歐盟要求會員國應有個資保護的專責機關，亞太鄰近先進國家亦於近年紛紛成立個資保護專責機關作為對內的個資保護監管執行機關及對外的個資保護交流窗口。

（2）強化國際合作與交流

在網路科技及電子商務的迅速發展下，個人資料的全球性流通已無法避免，是個人資料保護實亟需密切的跨國合作。如我國能有個資保護專責機關作為與他國聯繫之主體，不僅能降低交流難度，尚能促成更積極的個資保護國際合作，甚且作為加入個資保護國際組織的主體。

(二) 個資保護應有獨立性

歐盟對於會員國個資保護監督機關及 ICDPPC 對於申請加入會員的個資保護機關均要求具備「獨立性」，其中歐

盟更要求監督機關須有「完全之獨立性」(詳見本研究報告第二章第一節)。

此獨立性要求須彰顯於「組織」、「人事」、「功能」及「財務」等面向，並使個資保護專責機關在實質上「**得免於直接或間接受到來自外部的任何影響，以致使其執行職務有偏頗之虞**」(詳見本研究第二章第十五節)。

因此，成立個資保護專責機關，除應有前述「專責性」外，更應具備足夠的「獨立性」，是如僅由行政機關的內部單位職司個資法的監管執行，雖可具有專責性，但恐因「欠缺獨立性而無法免於直接或間接受到來自外部的任何影響，以致使其執行職務有偏頗之虞」；至若個資保護專責機關隸屬於上級機關之下，雖然有獨立的組織法規且原則上享有單獨的人員編制與預算[575]，但在「人事獨立性」部分恐略有不足，見下述。

(三) 個資保護專責機關之地位

1、不適宜作為行政法人

由於我國《行政法人法》第 2 條規定我國行政法人僅能執行符合「具有專業需求或須強化成本效益及經營效能者」、「不適合由政府機關推動，亦不宜交由民間辦理者」、「所涉公權力行使程度較低者」等條件之特定公共事務，然考量個資法之監管需要高度公權力

[575] 如上研究發現，歐盟 GDPR 對於監督機關的財務獨立性要求在於確保監督機關具備足夠之經費以執行職務，並不至因預算控管而影響其執行職務的客觀、公正，是如我國成立個資保護專責「機關」，應即符合 GDPR 的要求。

的行使，是在我國法制下，個資保護專責機關似不宜如同英國或香港般居於半官方的行政法人地位。

2、不適宜隸屬於總統

又考量我國政府體制的獨特性及行政效率的彰顯，個資保護專責機關應亦不宜如同南韓或澳門般直屬於最高（行政）首長。

3、二級或三級中央行政機關的獨立性存有爭議

雖然研究對象中的日本、新加坡、馬來西亞、菲律賓等國分將個資保護專責機關設為二級機關（例如我國行政院轄下一委員會）或三級機關（例如我國行政院法務部轄下一署），但由於**我國行政機關首長不享有任期保障，恐削減其人事上的獨立性；且在行政一體的監督下，亦難避免個資保護專責機關成員在執行職務時，存有受到上級長官、機關指示而影響其決定之客觀、公正性之虞，亦有損其功能上的獨立性**。

且依我國《中央行政機關組織基準法》規定，二級及三級行政機關之數量均有限制[576]，且依目前政府規劃均已達到上限。因此我國個資保護專責機關似不宜設為中央二級或三級行政機關。

4、成立獨立機關之可行性？

[576] 中央行政機關組織基準法，第 29 條第 2 項，「部之總數以十四個為限」；第 31 條第 2 項，「第一項委員會之總數以八個為限」；第 33 條第 3 項，「第一項及第三項署、局之總數除地方分支機關外，以七十個為限」。

如將我國個資保護專責機關設為《中央行政機關組織基準法》第 3 條第 2 項的「獨立機關」[577]，**不僅有獨立的「組織」法規及「財務」資源，在「功能」上亦是依法獨立行使職權，不受其他機關指揮監督，且在「人事」層面，獨立機關合議制之委員亦能依法享有任期保障**。

不過由於《中央行政機關組織基準法》第 32 條第 2 項規定我國相當二級機關之獨立機關數量以 3 個為限，目前已有中央選舉委員會、公平交易委員會及國家通訊傳播委員會等 3 個相當二級機關之獨立機關。如欲成立相當中央三級之獨立機關（如「飛航安全調查委員會」），或有設立空間，惟以三級獨立機關方式設立，是否能發揮部會協調之有效性，亦有疑慮。

須併予敘明者，由於依前述《中央行政機關組織基準法》第 3 條第 2 項規定，我國獨立機關應為「合議制」機關，其決策需由委員作成決議，因此在行政效率上是否將可能產生阻礙，應仍一併考量[578]。

二、監管對象與主管法規

由於個資法規範之對象包含公務機關及非公務機關，是我國如成立個資保護專責機關以執行實施個資法，則其監管對象亦應

---

[577] 中央行政機關組織基準法，第 3 條第 2 款，「本法用詞定義如下：二、獨立機關：指依據法律獨立行使職權，自主運作，除法律另有規定外，不受其他機關指揮監督之合議制機關」。

[578] 本研究期末審查委員提出參考「中央銀行」設置模式之意見亦值參考，該機關隸屬於行政院，雖非中央行政機關組織基準法下的獨立機關，但亦具備組織、人事、功能及財務上的獨立性，且屬「首長制」（總裁），惟其任務依該機關性質並不包含執法裁罰，且在我國中央政府體制下尚屬特例，是個資保護專責機關是否適宜比照辦理，仍需斟酌。

以「包含公務機關及非公務機關」為宜，此亦符合多數國家的國際實踐。惟就監管公務機關部分，仍須配合我國行政體制而與監管非公務機關的強度有所差別。

至該個資保護專責機關主管之法規範圍，由於個資法為普通法之性質，在現行法律架構下，其他法律如就特殊事項涉有規範，即應從該法律（例如政府資訊公開法、檔案法等），且現實考量甫成立個資保護專責機關的效能與經驗，似仍以專管個資法為宜，但日後應可考量將與個人資料保護相關之特別法逐步納由個資保護專責機關管轄。

三、增修個資保護專責機關之法定職務

由本研究比較各國法例可知，各國個資或隱私保護專責機關之法定職務較我國個資法賦予中央目的事業主管機關之法定職務更為全面及詳細，以讓專責機關更能有效確保該國人民權利的保障。

據此，本研究認為，如我國改採設置個資保護專責機關以監管個資法的實施，應於個資保護專責機關的「組織法」中授予更全面的「法定任務」，另在「法定職權」方面，除現行個資法第 21 條至第 27 條之「執法權」已相對完整外，尚應於該法中增列專責機關特定職權。前述任務與職權應包含：

（一）指導

1、專責機關應提升人民對於個資保護的風險意識及當事人權利的內涵與重要性。

2、專責機關應提升個資蒐集者及受託者對於法定義務

的認知。

3、專責機關應隨時掌握與個資保護相關的技術或實務發展。

4、專責機關應主動提供或被動答覆人民關於個資法下的當事人權利相關資訊。

5、專責機關應主動對個資蒐集者或受託者提供法律遵循的實務指引。

6、專責機關應主動提供或被動答覆個資蒐集者或受託者就個資保護事項之諮詢。

（二）核准

專責機關應負責核准個資蒐集者或受託者跨境傳輸個人資料(如跨境傳輸個人資料之規定修正為「原則禁止、例外允許」，見本研究報告第三章)。

（三）申訴處理

專責機關應依法受理人民就個資保護事件的申訴，並於調查後回覆結果。

四、結論

綜上所述，參考各國立法例，成立個資專責機關似為目前國際發展趨勢，惟我國受限於目前中央機關組織基準法之限制，未來如政策規劃成立個資專責機關，除建議修正「中央機關組織基準法」有關組織規模之建制標準外，另依「中央機關組織基準法」

第 5 條第 3 項規定，原則不得以作用法規定機關之組織，因目前個資法性質為作用法，建議配套訂定個資專責機關之組織依據。

第三章 資料在地化規範

全球貿易市場隨著網路科技及電子商務發展，資料的「跨（國）境傳輸」已成常態。各國政府無論係考量「人民的個資與隱私保護」或「政府監管的有效性」甚或「國際貿易中的政治手段」，均對資料的跨境傳輸設有寬嚴不一的規範。

本研究著眼於「個人資料保護議題」，即將研究重點聚焦於「跨境傳輸個人資料的國際規範」，並依規範密度區分為較嚴格的「資料在地化政策」，即要求資料蒐集者不得在境外蒐集境內當事人之個人資料，亦即資料蒐集者如透過網路取得該國自然人個資，須在該國境內設置伺服器保存；以及較寬鬆的「跨境傳輸限制」，即限制境內的資料蒐集者將在境內蒐集之當事人個資傳輸至境外地區。

第一節 資料在地化政策

資料在地化政策係指政府要求資料蒐集者不得在境外蒐集境內當事人之個人資料，美國資訊技術產業協會（Information Technology Industry Council, ITI）曾於 2017 年整理全球資料在地化法律規範[579]，本研究略述如下：

一、中國《網絡安全法》

中國於 2017 年 6 月 1 日施行《網絡安全法》，該法第 37 條規定「關鍵信息基礎設施的運營者在中華人民共和國境內運營中收集和產生的個人信息和重要數據應當在境內存儲。因業務需要，確需向境外提供的，應當按照國家網信部門會同國務院有關部門

[579] 見 http://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures1-19-2017.pdf，最後到訪日為 107 年 1 月 16 日。

制定的辦法進行安全評估；法律、行政法規另有規定的，依照其規定」。

二、俄羅斯《資料在地化法》

俄羅斯於 2015 年施行《資料在地化法（Data Localization Law）》，該法要求對俄羅斯公民蒐集的所有個資均應儲存於俄羅斯境內。

三、印度《國家資料分享及存取政策》

印度 2012 年的《國家資料分享及存取政策（National Data Sharing and Accessibility Policy）》規定，使用公基金（public funds）作為財務來源而蒐集之資料均應儲存於印度境內。

四、印尼《資訊及電子交易法》

印尼 2012 年的《資訊及電子交易法（Information and Electronic Transaction Law）》規定，任何直接向消費者提供網路服務的企業，均應將其資料中心設置於印尼境內。

五、越南《資訊科技服務法》

越南《資訊科技服務法（Decree of Information Technology Services）》規定，任何提供不同網路服務之企業應至少於越南境內設置一台伺服器[580]。

[580] Vietnam , Decree of Information Technology Services , Article25.8, “To have at least one server system in Vietnam serving the inspection, supervision, storage, and provision of information at the request of competent state management agencies, and settlement of customers’ complaints about the service provision according to regulations of the Ministry of Information and Communications”.

六、國際組織與協議

相較於上述國家採行嚴格的資料在地化政策，區域間的國際組織基於「促進商業貿易發展」的立場，多認應有條件允許跨境傳輸個人資料，而不採資料在地化措施（見下節），例如：

（一）OECD

經濟合作暨發展組織（Organization for Economic Co-operation and Development，OECD）於 1980 年制頒《隱私保護暨個人資料跨境流通指引（OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data）》，並於 2013 年提出修正[581]，該指引即規定，在符合特定情形下，會員國便不應禁止個人資料的跨境傳輸

（二）ICDPPC

個資與隱私保護委員國際研討會 ICDPPC 曾於 2009 年在西班牙召開時做成「馬德里決議（Madrid Resolution）」[582]，公布《個資與隱私保護國際標準（International Standards on the Protection of Personal Data and Privacy）》，並於該標準中主張，在符合特定條件下，國家即應允許跨境傳輸個人資料。

（三）APEC

APEC 為促進經濟區內個人資料的自由流動，避免各

---

[581] 見 https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf，最後到訪為 106 年 9 月 17 日。

[582] http://www.privacyconference2009.org/media/Publicaciones/common/estandares_resolucion_madrid_en.pdf，最後到訪日為 106 年 9 月 18 日。

會員經濟體的隱私保護規範落差形成個資跨境流通的阻礙，並同時保障個資當事人權利，特制定「跨境隱私保護規則體系（Cross Border Privacy Regulation System）」。

（四）TPP

《跨太平洋夥伴協定（TPP）》第 14 章第 11 條第 2 項規定，如服務提供者為從事業務活動而需以電子方式跨境傳輸個人資料時，除非另有其他正當公共政策目的，締約國即應允許該跨境傳輸行為[583]；且第 13 條第 2 項亦強調，締約國不可要求服務提供者在從事業務活動時必須使用或建置位於締約國境內之電腦運算設施[584]。

七、我國法律與研究建議

（一）個人資料保護法

在個人資料的跨境傳輸方面，個資法並未採取資料在地化規範模式，而是於第 21 條規定「允許跨境傳輸個人資料」[585]，且是「原則允許，例外始限制或禁止」（見下節）。

（二）數位通訊傳播法草案

---

583 TPP, Article14.11.2, “Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person”.

584 TPP, Article14.13.2, “No Party shall require a covered person to use or locate computing facilities in that Party’s territoryas a condition for conducting business in that territory”.

585 個人資料保護法，第 21 條，「非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：一、涉及國家重大利益。二、國際條約或協定有特別規定。三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。四、以迂迴方法向第三國（地區）傳輸個人資料規避本法」。

草案第 21 條第 1 項規定「數位通訊傳播服務提供者對其位於我國境內之使用者，不得以不合營業常規之方式規避經由我國境內通訊傳播設施傳輸、接取、處理或儲存與使用者相關之數位訊息」，雖然條文係指服務提供者不得「以不合營業常規」之方式規避我國境內設施，**但曾有草案版本中的立法理由為**「為便利我國境內使用者於權利遭受侵害時得有效蒐集相關數位證據，且得依涉外民事法律適用法定其應適用之法律，爰規定數位通訊傳播服務提供者之使用者如於我國境內，其服務之提供**應以**藉由我國境內之通訊傳播設施處理、儲存與使用者相關之數位訊息為原則，不得有刻意規避（irregularly bypass）之情事」[586]。

惟或係考量該立法理由恐導致解釋為我國將採取「資料在地化」政策之爭議，**後續草案版本之立法理由已修改為**「為便利我國境內使用者於權利遭受侵害時得有效蒐集相關數位證據，且得依涉外民事法律適用法定其應適用之法律，爰於第一項規定數位通訊傳播服務提供者之使用者如於我國境內，其服務之提供**如係**藉由我國境內之通訊傳播設施處理、儲存與使用者，其傳遞之數位訊息不得有刻意規避(irregularly bypass) 之情事」[587]。

（三）研究建議

本研究認為，在全球電子商務時代，個人資料的自由

---

586 見 https://www.ncc.gov.tw/chinese/files/17010/3861_36826_170104_1.pdf，最後到訪為 107 年 1 月 16 日。

587 見 https://www.ey.gov.tw/DL.ashx?s=AA83E4E94234DACA5B47EE551B8E93E8D8A7C6B36269C2A19A9969FC379C95384DCA9DD6E7A6D7D0&u=%2fUpload%2fRelFile%2f3329%2f756148%2f8e907cb2-ba39-4197-bfbc-1cb3c301ae43.pdf，最後到訪為 107 年 3 月 8 日。

流通確有其必要性，且我國個資法亦明定該法之本旨包含「促進個人資料的合理利用」，加以多數國家及區域貿易國際組織之趨勢均不傾向以「資料在地化」方式嚴格禁止個資的跨境流通，況在執行層面似須偏向極權之政府體制方能有效實踐「資料在地化」政策。

因此，我國個資法應不宜導入「資料在地化」的規範，而應在「可允許跨境傳輸個資」的基礎上，調整現行規範內容，詳見下節。

第二節　跨境傳輸規範

一、歐盟

即將於 2018 年生效適用於歐盟各會員國的歐盟《個人資料保護規則（General Data Protection Regulation, GDPR）》就跨境傳輸個人資料仍承襲歐盟《個人資料保護指令》時的「許可／同意，例外允許」模式，在第 44 條至第 50 條規定禁止將境內個資傳輸至個資保護適足性不足，亦無安全維護措施，也不符合特定例外的境外第三國或位於第三國的跨國組織，簡要說明如下：

(一) 具備「適足性（個資保護）」要件

依 GDPR 第 45 條第 1 項規定，對於經過歐盟認定具備個人資料適足性（adequate level of protection）的國家/領土/第三國之處理部門（processing sector），可不須得到批准即可進行個人資料的跨境傳輸[588]。而依同條第 2 項規定，歐盟

[588] GDPR, Article45(1), "A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an

考量是否具備適足性之因素包含[589]：

1、依該國/國際組織之法律規範、專業規則與安全措施，當事人得要求行政或司法救濟之權利，特別針對居住在歐盟境內之個人。

2、設有確保遵循個資保護規則之獨立監督機關存在，以協助與提供諮詢讓當事人行使其權利。

3、該國/國際組織作出的國際承諾。

(二) 傳輸者採取適當安全維護

依 GDPR 第 46 條第 1 項規定[590]，控管者或受託者如能採取適當安全維護措施，並確保資料當事人行使權利及請求賠償的有效性，則仍可將個資傳輸至未經歐盟認定具備適足性的境外地區，無須得到主管機關的批准。前述適當安全維

---

adequate level of protection. Such a transfer shall not require any specific authorisation."

589 GDPR, Article45(2), "When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements: a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred; b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data."

590 GDPR, Article46(1), "In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available."

護包含[591]：

1、公務機關間存有具法律拘束力且可執行之辦法。

2、傳輸者與接受者間存有 GDPR 第 47 條規定的約束性企業規則（binding corporate rules），內容包含[592]：

---

[591] GDPR, Article46(2), "The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by: a) a legally binding and enforceable instrument between public authorities or bodies; b) binding corporate rules in accordance with Article 47; c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2); d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2); e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights."

[592] GDPR, Article47(2), "The binding corporate rules referred to in paragraph 1 shall specify at least: a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members; b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question; c) their legally binding nature, both internally and externally; d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules; e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules; f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage; g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14; h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling; i) the complaint procedures; j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group

（1）事業團體或參與共同經濟活動之企業團體與團體內成員之組織架構及聯絡方式。

（2）跨境傳輸之事實，包括個資類別、處理行為及目的、受影響之資料當事人類別及該境外地區為何。

（3）該規則具備內部及外部之拘束性。

（4）該規則適用各項個資保護原則，尤其是目的限制原則、資料最小化原則、儲存期間限制、資料品質、預設個資保護、處理個資法律依據、特種個資之處理、資料安全維護，及再次傳輸個資至不受約束性企業規則拘束之接受者的所需條件。

（5）資料當事人之權利及行使方式，包含 GDPR 第 22 條賦予拒絕受自動化決定之權、第 79 條規定得向主管監督機關及會員國之管轄法院提起申訴之權，以及因企業違反約束性企業規則而得受償之權。

（6）於會員國境內設有據點之控管者或受託者，應對未於歐盟境內設有據點之事業體內其他企業違反約束性企業規則之行為承擔責任；控管者或受託者僅

---

of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority; k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority; l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j); m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and n) the appropriate data protection training to personnel having permanent or regular access to personal data.”

在能舉證證明該其他企業無須對損害負責時，始得免除全部或部分責任。

（7）如何將約束性企業規則之相關資訊，尤其是前述 4、5、6 款之內容，提供予資料當事人。

（8）依 GDPR 第 37 條指派之個資保護長的任務，或任何其他負責監督事業團體或參與共同經濟活動之企業團體是否遵守約束性企業規則及監督教育訓練與申訴處理之第三人或機關。

（9）申訴程序。

（10）事業團體或參與共同經濟活動之企業團體採取確保遵守約束性企業規則之驗證機制。該機制須包含個資保護稽核及確保採取足以保障資料當事人權利的矯正措施之方法。前述驗證結果應告知本項 8 款之人或機關，以及事業團體或參與共同經濟活動之企業團體的管理階層，且應依主管監督機關之要求提出。

（11）提報及記錄約束性企業規則之變更並將變更提報予主管監督機關之機制。

（12）與主管監督機關合作以確保事業團體或參與共同經濟活動之企業團體內所有成員均能遵守約束性企業規則之機制，特別是向主管監督機關提出本項 10 款的驗證結果。

（13）向主管監督機關報告事業團體或參與共同經濟

活動之企業團體內之成員，因第三國的法律要求而可能對約束性企業規則內保證之事項有重大不利影響之機制。

（14）對長期或常態性存取個資之人員提供的適當個資保護訓練。

3、傳輸者與接受者間簽訂依 GDPR 第 93 條第 2 項規定，經歐盟執委會採納或經歐盟執委會許可後由監督機關採納的標準個資保護條款（standard data protection clauses）[593]。

4、境外地區的接受者遵守依 GDPR 第 40 條規定許可的行為守則（code of conduct），並受有拘束力且可執行之協議規範須採取適當安全維護措施。

5、境外地區的接受者取得依 GDPR 第 42 條許可之認證（certification mechanism），並受有拘束力且可執行之協議規範須採取適當安全維護措施。

(三) 其他例外

依 GDPR 第 49 條第 1 項規定，如境外地區未具備歐盟認定之個資保護適足性，且傳輸者與接受者間又未符合適當安全維護之規定，則僅在下列情形之一時，始得將個資傳輸

[593] 標準個資保護條款於歐盟個資保護指令 95/46/EC 即已存在，分別為「控管者與控管者間」及「控管者與受託者間」之標準條款，內容略包含：1、名詞定義；2、傳輸者之義務；3、接受者之義務；4、賠償責任；5、當事人權利；6、準據法；7、爭議解決機制；8、契約終止效果；9、契約條款變更效力；10、傳輸內容描述；11、與監督機關合作事項；12、複委託規範。

至境外[594]：

1、 資料當事人經告知個資傳輸至該不具備適足性之地區且無適當安全維護措施所可能帶來的風險後，明確表示同意。

2、 該傳輸係為履行資料當事人與控管者間之契約所必要，或是應當事人的要求，為締結契約之準備行為所必要。

3、 該傳輸是為資料當事人之利益，履行控管者與第三人間之契約所必要。

4、 該傳輸係為重大公共利益所必要。

5、 該傳輸係為建構、行使或防禦法律上請求所必要。

6、 該傳輸係依據法規須提供給公眾之資訊，並公開給一般大眾或是有合法利益之人查詢，但僅及於該個案符合法定之查詢條件的範圍內。

[594] GDPR, Article49(1), "In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; d) the transfer is necessary for important reasons of public interest; e) the transfer is necessary for the establishment, exercise or defence of legal claims; f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case."

(四) 主管機關合作

執委會與監督機關應採取適當行動合作保護個資，例如發展跨國合作機制來促使個資保護之執行等。

(五) 歐美隱私盾（Privacy Shield）

值得注意的是，歐盟執委會本在 2000 年承認美國商業部的安全港隱私原則（Safe Harbor Privacy Principles）滿足指令要求的「適足性」要件，使得導入該原則的美國企業得以從歐盟境內取得個人資料。

然而，安全港隱私原則制定已逾 10 餘年，歐盟執委會本即已在檢討該原則的調整必要，歐洲法院更在 2015 年的 Facebook 案中宣告安全港隱私原則無效。因此歐盟執委會遂再與美國商業部協商，於 2016 年 7 月正式公布了歐盟執委會承認的個資保護適足性要件「隱私盾（Privacy Shield）」。其重要原則列示如下：

1、 告知義務

此原則規範資料控制者的應告知事項及告知時機，包含蒐集的個資類別、蒐集目的、遵守隱私盾的承諾、當事人權利及行使管道、擬揭露個資的對象及目的、當事人得限制資料使用或揭露的選擇權與行使方式、該資料控制者受到美國相關主管機關管理等。

2、 當事人選擇權

此原則要求資料控制者提供當事人選擇拒絕

（Opt-Out）「資料被揭露予第三人」或「資料被用於與原始蒐集目的重大不符之新目的」的權利。

3、傳輸資料責任

如資料控制者欲將個資傳輸予第三人，須遵守前述告知義務與當事人選擇權原則，並應以契約要求該第三人僅得於當事人同意的特定目的限制內使用當事人個資，且要求第三人以同樣程度遵守隱私防衛原則。

如資料控制者欲將個人資料傳輸予受託處理個資的資料處理者時，資料控制者僅得在原始蒐集個資之目的限制內為之，且須確保受託者的個資保護措施應至少遵守隱私盾規範，並應採取合理的適當措施監督受託者是否遵守規範。

4、安全維護

此原則要求資料控制者採取合理而適當之安全維護措施以避免個資侵害事故的發生。

5、個資品質與目的限制

此原則要求資料控制者僅得於蒐集個資之目的內使用當事人的個人資料，且資料控制者應採取合理步驟確保當事人個資的完整、正確與即時。

6、當事人近取權

此原則要求資料控制者確保當事人得行使其更正、

刪除個資等當事人權利。

(六) 約束性企業規則（Binding Corporate Rules）

對於跨國企業集團而言，由於本質上即須經常性、頻繁性將企業所保有的個人資料傳輸至位於境外國家的集團內其他企業，因此如須根據每次或針對每種類型的特定個人資料傳輸重新決定是否合法，在實務面將有窒礙難行的繁瑣之處。因此歐盟個資保護規則提供一項「約束性企業規則」方案，讓跨國企業可基於集團內的業務需求，自由地將個人資料國際傳輸至位於境外的集團內其他企業，無須逐次確認有無符合該指令規範的例外要件，也無須在集團內各企業公司間簽署多份契約。

約束性企業規則由需求集團位於歐盟的總部企業或授權一間於歐盟的代表企業，依照歐盟個人資料保護指令第 29 條工作小組要求的必要內容自行撰擬，並向該國的主管機關申請批准。必要內容包含：

1、個人資料的傳輸

規則內應對個人資料的國際傳輸具體說明，使主管機關能據以評估境外的資料接受國對於個人資料的保護是否適足。

2、個資保護的安全措施

規則內應載明該跨國企業集團對於個人資料的安全維護，以確保對於個人資料之蒐集、處理、利用的透明性、公平性、目的限制性及當事人權利和個資安

全獲得保障。

3、變更規則的提報程序

規則內應明定如該規則的內容修正或集團內有重大變更事項（如集團內新增其他國家企業），致有影響該集團對於個資保護法令遵守有重要影響時，須向主管機關提報的程序。

4、確保各企業遵守規則的內控制度

規則內應規範該集團確保內部各企業瞭解並遵守規則的內部控制制度，包含人員管理、教育訓練、獎懲措施等。

5、稽核制度

規則內應訂定集團各企業對於規則遵守及個資保護的內部稽核或外部稽核制度，定期由合格的專業人員進行稽核。並應提交稽核計劃予主管機關，且允許主管機關對集團企業進行稽核。

6、申訴處理制度

規則內應建立當事人權利的行使管道及完整的申訴處理制度。

7、與主管機關配合

規則內應承諾該集團負擔與主管機關配合的義務，包含同意接受主管機關的稽核及各企業須明確同意遵守主管機關針對個資保護提出的建議。

8、司法管轄

規則內應記載該集團同意當事人得在下列管轄區對企業提起訴訟：

(1) 最初國際傳輸個人資料的企業所在管轄區。

(2) 該集團的歐洲總部企業所在管轄區或代表集團的歐洲境內企業所在的管轄區。

9、當事人救濟

規則內須載明該集團對於企業違反規則導致當事人受有損害時的賠償制度，包含對於歐盟境外的集團企業所造成的損害向當事人給付賠償金。

10、責任

位於歐洲的總部企業或代表集團的歐洲企業須對境外的其他集團企業之行為負責，如該境外的企業遭指控違反規則，總部企業或代表企業須舉證證明該事實之有無。

11、促進規則公開

規則內應有具體方式促進此規則對當事人公開，使當事人能隨時獲取該規則之內容。

12、規則的約束性

為強化此規則在集團內執行上的拘束性，規則應說明集團促使各企業遵守規則的強制性，方式包括：

(1) 對有關人員進行規則內容的認知教育訓練。

(2) 對違反規則的員工予以懲處。

(3) 健全的申訴處理制度。

(4) 完整的內部稽核程序。

(5) 違反規則的救濟制度。

(6) 當事人有權提請主管機關審查規則的遵守。

指定個資保護專責人員。

(七) 標準個資保護契約條款

如前所述，即便資料接受國未被歐盟執委會認定符合「適足性（個資保護）」條件，資料提供者仍能在符合特定例外下國際傳輸個人資料至位於該國的資料接受者，而雙方簽訂「標準個資保護契約條款」即為適例，簡要說明如下：

1、 標準個資保護契約條款概述

標準個資保護契約條款由歐盟執委會制頒，現行有效版本計有三份，依資料提供者及資料接受者的身分而區分為：

(1) 資料控制者與資料控制者（2001、2004）：適用於資料提供者及資料接受者均對所欲傳輸的個人資料具有實際控制需求，雙方皆具有各自的特定目的而蒐集、處理、利用當事人個人資料的情形。

(2) 資料控制者與受託之資料處理者（2010）：適用於資

料接受者係代資料提供者處理個人資料之情形，即僅資料提供者為實際控制該個人資料之主體，資料接受者是為資料提供者的特定目的而處理、利用當事人的個人資料。

上述兩種標準個資保護契約條款各有其規範目的，最重要的區別在於資料接受者如為受託之資料處理者時，應受資料提供者的目的限制，不可為自己的目的而使用當事人之個人資料，且在契約關係結束後，資料接受者應依資料提供者的要求將該個人資料返還或刪除、銷毀。

因此兩種標準個資保護契約條款不可混淆，且如欲以標準個資保護契約條款作為例外國際傳輸個人資料的合法要件時，資料提供者及資料接受者均不可增減或修改標準個資保護契約條款之內容。

至於標準個資保護契約條款的內容則大抵列有：1、名詞定義；2、資料提供者之義務；3、資料接受者之義務；4、賠償責任；5、當事人權利；6、準據法；7、爭議解決機制；8、契約終止效果；9、契約條款變更效力；10、傳輸內容描述；11、與主管機關合作事項；12、複委託規範。

2、 標準個資保護契約條款簽訂模式

由於企業常須將個人資料提供給數個資料接受者，或企業常須從數個資料提供者取得個人資料，為使標準

個資保護契約條款具體發揮成效，實務上約略發展出三種利用標準個資保護契約條款的簽訂來合法國際傳輸個人資料的模式[595]：

(1) 契約網路模式

此模式係指在所有資料提供者及資料接受者間均簽訂標準個資保護契約條款。優點在於確保任何資料提供者及資料接受者間均具有明確的法律關係，可於個資侵害事故或爭議發生時迅速釐清責任；缺點則是在同一商業行為涉及多數資料提供者及資料接受者時，可能存在大量的標準個資保護契約條款，對於任一資料提供者或資料接受者都將帶來執行上的負擔。

(2) 主契約模式

此模式係指同一商業行為中的所有資料提供者及資料接受者均簽訂「同一份」標準個資保護契約條款。優點在於任一資料提供者或資料接受者皆僅須管理及執行一份標準個資保護契約條款以確保自己的行為合於條款內容即可，且如有新增資料提供者或資料接受者時，只須在該份標準個資保護契約條款後增補簽名，無須另行簽訂契約；缺點則是同一企業在同一商業行為中，可能同時是資料提供者也是資料接受者，簽訂標準個資保護契約條款

[595] 參原著：（德）Chrstopher Kuner，譯者：旷野、杨会永等（2008），*欧洲数据保护法：公司遵守与管制*，中國法律出版社，p215-219。

的身分有時不易區分。

(3) 授予代理權模式

此模式係指在同一商業行為中，由參與行為的資料提供者授予代理權給另一資料提供者，或由資料接受者授予代理權給另一資料接受者，由獲得代理權的資料提供者與資料接受者簽訂標準個資保護契約條款。優點是可簡化所有參與此商業行為的資料提供者與資料接受者間的法律關係；缺點則在於代理權授予的內部關係（如授權條件、權利限制等）易生爭議。

二、英國

英國個人資料保護法於附表1第1部份第8原則對跨境傳輸個人資料採原則禁止、例外允許模式，規定「個人資料不應被傳輸至歐洲經濟區以外的國家或地區，除非該國家或地區保證對資料當事人關於個人資料處理之權利與自由有適當程度的保護」[596]。其所稱「適當程度的保護」係指審酌下列事項後，在具體情況中具備適足性[597]：

---

[596] UK, Data Protection Act, Schedule1, Part1, 8, "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data".

[597] UK, Data Protection Act, Schedule1, Part2, 13, "An adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to—(a)the nature of the personal data,(b)the country or territory of origin of the information contained in the data,(c)the country or territory of final destination of that information,(d)the purposes for which and period during which the data are intended to be processed,(e)the law in force in the country or territory in question,(f)the international obligations of that country or territory,(g)any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases), and(h)any security measures taken in respect of the data in that

(一) 個人資料的性質。

(二) 該資料所含原始資訊來源之國家或地區。

(三) 最終接收該資訊的國家或地區。

(四) 處理個人資料的目的及期間。

(五) 系爭接收國家或地區的相關法律。

(六) 系爭接收國家或地區應遵守的國際義務。

(七) 任何在系爭接收國家或地區生效的實務指引或其他規則。

(八) 系爭接收國家或地區對接收之個人資料採取的任何安全維護措施。

然而，如符合英國個人資料保護法附表 4 所列情形，則前述第 8 原則即不適用（個人資料得傳輸至歐洲經濟區以外之國家或地區），除非內閣大臣另有相反命令[598]：

(一) 資料當事人同意該跨境傳輸[599]。

(二) 該跨境傳輸是為完成資料控制者與資料當事人間的契約所必要；或是依資料當事人要求，為與資料控制者成立契約所必要[600]。

(三) 該跨境傳輸是「資料控制者為與第三人締結契約所必要，且

---

country or territory".

598 UK, Data Protection Act, Schedule1, Part2, 14, "The eighth principle does not apply to a transfer falling within any paragraph of Schedule 4, except in such circumstances and to such extent as the Secretary of State may by order provide".

599 UK, Data Protection Act, Schedule4, 1, "The data subject has given his consent to the transfer".

600 UK, Data Protection Act, Schedule4, 2, "The transfer is necessary—(a)for the performance of a contract between the data subject and the data controller, or(b)for the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller".

該第三人係受資料當事人要求締結契約或該契約對資料當事人有利」或「為履行前述契約所必要」[601]。

(四) 該跨境傳輸是為重大公共利益所必要。內閣大臣得以命令指明所稱「重大公共利益」之情形[602]。

(五) 該跨境傳輸是為完成法律程序所必要、為獲得法律建議所必要，或為確認、行使法律權利或辯護權利所必要[603]。

(六) 該跨境傳輸係為保護資料當事人的重大利益所必要[604]。

(七) 該跨境傳輸之個資係公開登記之個人資料，且查詢該個資的（境外）個資接受者已遵守查閱個資的所有條件[605]。

(八) 該跨境傳輸係由資訊委員確認對資料當事人的權利與自由均有適當安全維護後所允許[606]。

(九) 該跨境傳輸係由資訊委員授權以能確保資料當事人的權利

---

601 UK, Data Protection Act, Schedule4, 3, "The transfer is necessary—(a)for the conclusion of a contract between the data controller and a person other than the data subject which—(i)is entered into at the request of the data subject, or(ii)is in the interests of the data subject, or(b)for the performance of such a contract".

602 UK, Data Protection Act, Schedule4, 4, " (1)The transfer is necessary for reasons of substantial public interest.(2)The [F1 Secretary of State] may by order specify—(a)circumstances in which a transfer is to be taken for the purposes of sub-paragraph (1) to be necessary for reasons of substantial public interest, and(b)circumstances in which a transfer which is not required by or under an enactment is not to be taken for the purpose of sub-paragraph (1) to be necessary for reasons of substantial public interest".

603 UK, Data Protection Act, Schedule4, 5, " The transfer—(a)is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),(b)is necessary for the purpose of obtaining legal advice, or(c)is otherwise necessary for the purposes of establishing, exercising or defending legal rights".

604 UK, Data Protection Act, Schedule4, 6, "The transfer is necessary in order to protect the vital interests of the data subject".

605 UK, Data Protection Act, Schedule4, 7, "The transfer is of part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data are or may be disclosed after the transfer".

606 UK, Data Protection Act, Schedule4, 8, "The transfer is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects".

與自由均有適當安全維護之方式所為[607]。

三、加拿大

加拿大個資保護及電子文件法對於個人資料的傳輸並未區分境內或境外，在附表 1 的 4.1.3 條規定持有個人資料之組織應負責保障其所持有及管理的個人資料，並應採用契約或其他方式確保傳輸給第三方的個人資料可受到相當程度的安全維護措施的保護[608]。

在此同時，加拿大隱私委員辦公室亦於 2009 年發布《跨境處理個資指引（Processing Personal Data Across Borders Guidelines）》[609]，指導個資傳輸者應採取何種作為以確保跨境傳輸個人資料符合法律規範，簡要說明內容如下：

(一) 相同層級保護

個資傳輸者應確保境外的個資接受者能對當事人提供相同層級的個資保護。

(二) 簽署契約

個資傳輸者與個資接受者應透過契約約束權利義務以確保當事人權利獲得足夠保障。

---

607 UK, Data Protection Act, Schedule4, 9, "The transfer has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects".

608 Canada, Personal Information Protection and Electronic Documents Act, Schedule1, 4.1.3, " An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

609 見 https://www.priv.gc.ca/media/1992/gl_dab_090127_e.pdf，最後到訪為 106 年 9 月 15 日。

(三) 合理措施

個資傳輸者應採取一切合理措施來確保當事人的個資不會遭個資接受者未經授權下而使用或揭露。

雙方應於契約中約定個資接受者須制定相關的隱私保護政策及管理程序，包括人員訓練及安全維護措施，以保護當事人個資的安全。而個資傳輸者亦應有權對個資接受者進行稽核及調查。

(四) 風險評估

個資傳輸者在跨境傳輸個人資料前應先進行個資完整性、安全性及機密性的風險評估。

(五) 資訊透明

個資傳輸者應將跨境傳輸個人資料的相關資訊透明化，例如以適當方式明確讓當事人知悉其個人資料將基於何種目的被傳輸予境外地區的個資接受者。

四、香港

尚未實施的香港個人資料（私隱）條例第 33 條對於跨境傳輸個人資料採原則禁止、例外允許模式，規定除非符合下列條件，否則資料使用者不得將個人資料移轉至香港以外的地方[610]：

(一) 該地方經香港個人資料私隱專員有合理理由相信具備與條例大體上相似或達成與條例相同目的之法律正在生效，並藉

[610] 香港，個人資料(私隱)條例，第 33 條第(2)款。

憲報公告指明該地方[611]。但專員如有合理理由相信該地方已不再具備前述生效之法律時，即須廢除或修訂該公告[612]。

(二) 該使用者有合理理由相信在該地方有與條例大體上相似或達成與條例相同目的之法律正在生效。

(三) 有關的資料當事人已以書面同意該項移轉。

(四) 該使用者有合理理由相信在有關個案的所有情況下：

1、該項移轉是為避免針對資料當事人的不利行動或減輕該等行動的影響而作出。

2、獲取資料當事人對該項移轉的書面同意不切實可行。

3、如獲取書面同意是切實可行的，則資料當事人會給予上述同意。

(五) 該個人資料依條例第8部規定而豁免不適用條例附表1保障資料原則的第3原則「個人資料的使用」規定[613]。

(六) 若該資料在香港以某方式收集、持有、處理或使用，便會違反條例規定，而該使用者已採取所有合理的預防措施及已作出所有應作出的努力，以確保該資料不會在該地方以該方式

---

611 香港，個人資料(私隱)條例，第33條第(3)款，「凡專員有合理理由相信在香港以外的某地方有與本條例大體上相似或達致與本條例的目的相同的目的之法律正在生效，他可藉憲報公告，為本條的施行指明該地方」。

612 香港，個人資料(私隱)條例，第33條第(4)款，「凡專員有合理理由相信在第(3)款下的公告所指明的某地方，已不再有與本條例大體上相似或達致與本條例的目的相同的目的之法律正在生效，他須藉廢除或修訂該公告，令該地方停止被為本條的施行而指明」。

613 指香港個人資料(私隱)條例第51A條「執行司法職能」、第52條「家居用途」、第57條「關於香港的保安等」、第58條「罪行等」、第58A條「《截取通訊及監察條例》所指的受保護成果及有關紀錄」、第59條「健康」、第59A條「未成年人的照顧及監護」、第60B條「法律程序等」、第61條「新聞」、第62條「統計及研究」、第63B條「盡職調查」、第63C條「危急處境」、第63D條「轉移紀錄予政府檔案處」。

收集、持有、處理或使用。

五、澳門

澳門個人資料保護法對於跨境傳輸個人資料採原則禁止、例外允許模式，在第 19 條第 1 款規定「僅得在遵守本法律規定，且接受轉移資料當地的法律體系能確保適當的保護程度的情況下，方可將個人資料移轉到特區以外的地方」[614]，而前述法律體系能否確保適當的保護程度係由澳門個人資料保護辦公室（公共當局）作出決定[615]，須就跨境傳輸的所有情況或跨境傳輸資料的整體進行審議，並考量下列事項[616]：

(一) 資料的性質。

(二) 處理資料的目的、期間或處理計劃。

(三) 資料來源地和最終目的地。

(四) 有關法律體系現行的一般或特定的法律規則。

(五) 所遵守的專業規則和安全措施。

惟雖該澳門特區以外的地方的法律體系無法確保達到前述適當的保護程度時，如符合下列情形之一者，仍得將個人資料傳輸至澳門境外[617]：

(一) 資料當事人明確同意。

---

[614] 澳門，個人資料保護法，第 19 條第 1 款。
[615] 澳門，個人資料保護法，第 19 條第 3 款。
[616] 澳門，個人資料保護法，第 19 條第 2 款。
[617] 澳門，個人資料保護法，第 20 條第 1 款。

(二) 該跨境傳輸為執行資料當事人和負責處理個人資料的實體間的契約所必須，或是應資料當事人要求執行訂定契約的預先措施所必須者。

(三) 該跨境傳輸為執行或訂定依契約所必需，而該契約係為資料當事人之利益由負責處理個人資料的實體和第三人間所訂立或將訂立者。

(四) 該跨境傳輸係為保護重要的公共利益，或是在司法訴訟中宣告、行使或維護權利所必需或法律要求者。

(五) 該跨境傳輸是保護資料當事人的重大利益所必需。

(六) 該跨境傳輸是在公開登記後進行，且依據法律或行政法規，該登記是為公眾資訊和可供一般公眾或證明有正當利益之人公開查詢之用，只要在具體性況下遵守上述法律或行政法規訂定之查詢條件。

(七) 負責處理個人資料的實體確保具有足夠保障他人的私生活、基本權利和自由的機制，尤其透過適當的契約條款確保上述權利的行使，則澳門個人資料保護辦公室（公共當局）得許可跨境傳輸[618]。

又如個人資料的轉移係維護公共安全、預防犯罪、刑事偵查和制止刑事違法行為及保障公共衛生所必要的措施時，個人資料的跨境傳輸應由澳門的專法或適用於澳門的國際性文書以及區際協定規範[619]。

---

[618] 澳門，個人資料保護法，第 20 條第 2 款。
[619] 澳門，個人資料保護法，第 20 條第 3 款。

六、日本

日本個人情報保護法第 24 條規定，除將個人資料傳輸至經日本個人情報保護委員會以法令認定具備與日本相稱的個資保護體系，足以保護資料當事人的權利與利益的國家或地區外，非公務機關須事先得到資料當事人同意，始得將資料當事人的個人資料傳輸至位於日本境外之國家或地區的第三方。但符合日本個人情報保護法第 23 條第 1 項所列下述情形不在此限：

(一) 依法規規定須跨境傳輸。

(二) 為保護他人生命、身體、財產所須，且難以得到資料當事人的同意。

(三) 為增進公共衛生或促進兒童健全育成所須，且難以得到資料當事人的同意。

(四) 為協助中央或地方公務機關（包含受其委託之人）執行法定職務，且若經當事人同意則有可能妨害該法定職務之執行。

七、南韓

南韓個人資訊保護法（Personal Information Protection Act）對於跨境傳輸個人資料採原則禁止、例外允許模式，在第 17 條第 3 項規定「資料處理者須先向資料當事人告知法定事項並取得同意後，始得將其個資傳輸至南韓境外」[620]。前述法定事項包含

[620] South Korea, Personal Information Protection Act, Article17(3), "When the personal information processor provides personal information to a third partyoverseas, it shall inform data subjects of any of Subparagraphs of Paragraph (2), andobtain consent from data subjects".

[621]：

(一) 個人資訊接收者。

(二) 個人資訊接收者利用個人資料之目的。

(三) 跨境傳輸的個資項目（particulars）。

(四) 個人資訊接收者保存及利用個人資訊的期間。

(五) 資料當事人得拒絕同意及不同意對其有何不利影響。

八、新加坡

新加坡個人資料保護法對於跨境傳輸個人資料採原則禁止、例外允許模式，在第 26 條規定「除非遵守本法要求的條件以確保組織提供標準的個資保護措施使傳輸個資的保護措施與本法相當，否則組織不得將個人資料傳輸至新加坡境外國家或地區」[622]。

但資訊委員會得經組織申請，以書面通知豁免前述限制[623]，該豁免得附加條件且不須刊登於新加坡公報，並得隨時由資訊委員會撤銷[624]。又資訊委員會得隨時增加、變更或撤銷本條規定下

---

[621] South Korea, Personal Information Protection Act, Article17(2), "...1. The recipient of personal information;2. The purpose of use of personal information of the said recipient;3. Particulars of personal information to be provided;4. The period when personal information is retained and used by the said recipient; and5. The fact which data subjects are entitled to deny consent, and disadvantage affectedresultantly from the denial of consent".

[622] Singapore, Personal Data Protection Act2012, Section26(1), "An organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act".

[623] Singapore, Personal Data Protection Act2012, Section26(2), "The Commission may, on the application of any organisation, by notice in writing exempt the organisation from any requirement prescribed pursuant to subsection (1) in respect of any transfer of personal data by that organisation".

[624] Singapore, Personal Data Protection Act2012, Section26(3), "An exemption under subsection

的任何條件[625]。

九、馬來西亞

馬來西亞個人資料保護法對於跨境傳輸個人資料採原則禁止、例外允許模式，在第 129 條規定「資料使用者禁止將個資傳輸至馬來西亞境外地區，除非該地區經部長在資訊委員的建議下指明許可接受傳輸並公告於馬來西亞公報」[626]。

前述得經部長指明許可接受傳輸之境外地區的條件為下列情形之一[627]：

(一) 該地區具有與馬來西亞個人資料保護法大致相仿或有相同目的之現行法律。惟如資訊委員有合理根據相信前述條件已經消失，即應向部長提出建議，由部長取消或變更公告，使該地區不再成為可接收跨境傳輸個人資料之境外地區。資料使用者應於公告之日即停止傳輸個人資料至該境外地區[628]。

---

(2) —(a)may be granted subject to such conditions as the Commission may specify in writing; and(b)need not be published in the Gazette and may be revoked at any time by the Commission".

625 Singapore, Personal Data Protection Act2012, Section26(4), "The Commission may at any time add to, vary or revoke any condition imposed under this section".

626 Malaysia, Personal Data Protection Act 2010, Section129(1), " A data user shall not transfer any personal data of a data subject to a place outside Malaysia unless to such place as specified by the Minister, upon the recommendation of the Commissioner, by notification published in the Gazette".

627 Malaysia, Personal Data Protection Act 2010, Section129(2), "For the purposes of subsection (1), the Minister may specify any place outside Malaysia if— (a) there is in that place in force any law which is substantially similar to this Act, or that serves the same purposes as this Act; or (b) that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by this Act".

628 Malaysia, Personal Data Protection Act 2010, Section129(4), "Where the Commissioner has reasonable grounds for believing that in a place as specified under subsection (1) there is no longer in force any law which is substantially similar to this Act, or that serves the same purposes as this Act— (a) the Commissioner shall make such recommendations to the Minister who shall, either by cancelling or amending the notification made under subsection (1), cause that place to cease to be a place to which personal data may be transferred under this section; and (b) the data user shall cease to transfer any personal data of a data subject to such place with effect from the time as specified

(二) 該地區確保對於個人資料的處理行為具備至少與馬來西亞個人資料保護法規定的個資保護程度相稱的適當安全維護程度。

如不符合上述要求，但符合下列情形之一時，資料使用者亦得將個人資料跨境傳輸至馬來西亞境外地區[629]：

(一) 資料當事人同意該跨境傳輸。

(二) 該跨境傳輸是為執行資料當事人與資料使用者間的契約所必需。

(三) 該跨境傳輸係資料使用者為與第三人締結契約所必要，且該第三人係受資料當事人要求締結契約或該契約對資料當事人有利。

(四) 該跨境傳輸是為進行法律程序、獲得法律建議，或為確認、行使法律權利或辯護權利。

(五) 資料使用者有合理依據相信：

---

by the Minister in the notification".

[629] Malaysia, Personal Data Protection Act 2010, Section129(3), "Notwithstanding subsection (1), a data user may transfer any personal data to a place outside Malaysia if— (a) the data subject has given his consent to the transfer; (b) the transfer is necessary for the performance of a contract between the data subject and the data user; (c) the transfer is necessary for the conclusion or performance of a contract between the data user and a third party which— (i) is entered into at the request of the data subject; or (ii) is in the interests of the data subject; (d) the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights; (e) the data user has reasonable grounds for believing that in all circumstances of the case— (i) the transfer is for the avoidance or mitigation of adverse action against the data subject; (ii) it is not practicable to obtain the consent in writing of the data subject to that transfer; and (iii) if it was practicable to obtain such consent, the data subject would have given his consent; (f) the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of this Act; (g) the transfer is necessary in order to protect the vital interests of the data subject; or (h) the transfer is necessary as being in the public interest in circumstances as determined by the Minister".

1、該跨境傳輸是為避免或減輕對資料當事人的不利行為。前述不利行為係指損及資料當事人的權利、利益、特權、義務等行為[630]。

2、難以得到資料當事人對該跨境傳輸的書面同意。

3、如得到資料當事人的同意係確實可行，則該資料當事人必然同意該跨境傳輸。

(六) 資料使用者已採取所有合理預防措施並執行所有盡職調查以確保該個人資料在境外不會被以違反馬來西亞個人資料保護法規定的任何方式處理。

(七) 該跨境傳輸是為保護資料當事人的重大利益所必要。

(八) 該跨境傳輸是經部長決定為公共利益所必需。

十、菲律賓

菲律賓資料隱私法對於個人資料的傳輸並未區分境內或境外，在第 21 條規定「資料控制者應對其控制或保有的個資負責，包含傳輸給第三方的個人資料，無論是在境內的第三方或依跨境協議或合作而在境外的第三方」[631]。

依菲律賓資料隱私法規定，資料控制者有遵守該法各項要求之義務，並應以契約或其他合理方式控管接收個人資料之第三方

---

[630] Malaysia, Personal Data Protection Act 2010, Section129(6), "For the purposes of this section, “adverse action”, in relation to a data subject, means any action that may adversely affect the data subject’s rights, benefits, privileges, obligations or interests".

[631] Philippines, Data Privacy Act of 2012, Section21, "Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation".

亦能以相當程度的安全維護措施保護由資料控制者傳輸之個人資料[632]。資料控制者應指派一人或數人作為遵循菲律賓資料隱私法的專責人員，並須在資料當事人要求時告知該專責人員之身分[633]。

十一、紐西蘭

紐西蘭隱私法對於跨境傳輸個人資料採原則允許、例外禁止模式，在第 114B 條第 1 項規定「若資訊委員有合理根據認為構成下列事項，得禁止將個人資料從紐西蘭傳輸至其他國家或地區：1、該個人資料已（或將）從他國或地區傳輸至紐西蘭，並有可能傳輸到未提供與紐西蘭隱私法相當的保護措施之第三國或地區，且 2、此傳輸可能導致違反規定於 OECD 第 2 部份的指導原則及紐西蘭隱私法附表 5A 之基本原則」[634]。但有下列情形之一時，不在此限[635]：

(一) 該跨境傳輸或該個人資料係受法規要求或授權。

---

632 Philippines, Data Privacy Act of 2012, Section21(a), "The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party".

633 Philippines, Data Privacy Act of 2012, Section21(b), "The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request".

634 New Zealand, Privacy Act1993, Section114B(1), "The Commissioner may prohibit a transfer of personal information from New Zealand to another State if the Commissioner is satisfied, on reasonable grounds, that—(a) the information has been, or will be, received in New Zealand from another State and is likely to be transferred to a third State where it will not be subject to a law providing comparable safeguards to this Act; and(b) the transfer would be likely to lead to a contravention of the basic principle sof national application set out in Part Two of the OECD Guidelines and set out in Schedule 5A".

635 New Zealand, Privacy Act1993, Section114B(3), "Subsection (1) does not apply if the transfer of the information, or the information itself, is—(a) required or authorised by or under any enactment; or(b) required by any convention or other instrument imposing international obligations on New Zealand".

(二) 該跨境傳輸或該個人資料係由拘束紐西蘭的國際協議或法律文書所要求。

資訊委員在決定是否禁止個人資料跨境傳輸時，除考量上述規定及紐西蘭隱私法第 14 條規定外，應一併審酌下列事項[636]：

(一) 該跨境傳輸是否或將會對資料當事人有所影響。

(二) 促進紐西蘭與該境外國家或地區間的資訊自由流通之益處。

(三) 任何既存或發展中與跨境個資流動相關的國際指引，包含但不限於：

1、OECD《隱私保護暨個人資料跨境流通指引（OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data）》隱私保護指導原則。

2、歐盟個人資料保護指令 95/46/EC[637]。

十二、經濟合作暨發展組織（OECD）

經濟合作暨發展組織（Organization for Economic Co-operation and Development，OECD）於 1980 年制頒《隱私

[636] New Zealand, Privacy Act1993, Section114B(2), "In determining whether to prohibit a transfer of personal information, the Commissioner must also consider, in addition to the matters set out in subsection (1)and section 14, the following:(a) whether the transfer affects, or would be likely to affect, any individual; and(b) the general desirability of facilitating the free flow of information between New Zealand and other States; and(c) any existing or developing international guidelines relevant to transborder data flows, including (but not limited to)—(i) the OECD Guidelines; (ii) the European Union Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data".

[637] 該指令將於 2018 年由歐盟個人資料保護規則(General Data Protection Regulation)取代。

保護暨個人資料跨境流通指引（OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data）》，並於 2013 年提出修正[638]。

(一) 隱私保護指導原則

該指引要求會員國應遵守下列隱私保護原則：

1、蒐集限制原則

取得個人資料須合法、公平且在必要範圍內為之，並須以適當方式向當事人告知或取得其同意。

2、資料品質原則

蒐集的個人資料應與所要利用的目的有正當合理的關聯，並且應保持個人資料的正確、完整及即時更新。

3、目的特定原則

應於取得資料時即特定蒐集個人資料的目的，且後續的利用個資行為均應合於蒐集時的特定目的。

4、使用限制原則

除非取得當事人的同意或是法律另有規定，不得於蒐集個人資料的特定目的外利用個人資料。

5、安全維護原則

[638] 見 https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf，最後到訪為 106 年 9 月 17 日。

應採取合理安全維護措施以防止個人資料遭遺失或未經授權的存取、毀損、使用、修正或揭露。

6、開放原則

個人資料的資訊應保持開放，相關政策應讓當事人能隨時知悉個資的性質、使用的目的以及蒐集機關的身分及所在地。

7、當事人參與原則

當事人有權向蒐集機關要求提供其個人資料或確認是否保有其個人資料；蒐集機關應有合理理由始得拒絕當事人行使前述權利，且應給予當事人申訴的機會。當事人亦有權向蒐集機關請求刪除、更正、補充或修改其個人資料。

8、責任原則

蒐集機關有義務採取有效的方式遵守前述各項原則。

(二) 例外限制跨境傳輸個人資料

OECD 鼓勵促進個人資料的自由跨境流通，因此本指引認為，在符合下列任一情況時，會員國即不應禁止個人資料的跨境傳輸[639]：

[639] OECD, Privacy Framework, Chapter1, Part4, 17, " A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines".

1、個資接受者的國家法規本質上符合前述隱私保護指導原則。

2、在個資傳輸過程中存有足夠的安全維護，包含有效的執行機制及適當措施以確保持續符合前述隱私保護指導原則之等級。

十三、個資與隱私保護委員國際研討會（ICDPPC）

個資與隱私保護委員國際研討會 ICDPPC 曾於 2009 年在西班牙召開時做成「馬德里決議（Madrid Resolution）」[640]，公布《個資與隱私保護國際標準（International Standards on the Protection of Personal Data and Privacy）》，其中第二部份揭示個資與隱私保護的 6 項原則，分別為：「合法及公平原則」、「目的特定原則」、「比例原則」、「資料品質原則」、「開放原則」、「責任原則」。並在第 15 條就「跨境傳輸個人資料」主張：

(一) 跨境傳輸個人資料之前提為個資接受國至少符合本標準所訂的個資保護水平[641]。

(二) 如個資接受國未符合前述個資保護水平，但個資傳輸者保證個資接受者能滿足本標準所訂的個資保護等級（例如適當的契約條款拘束，或跨國公司或跨國組織內部存有具強

640 http://www.privacyconference2009.org/media/Publicaciones/common/estandares_resolucion_madrid_en.pdf，最後到訪日為 106 年 9 月 18 日。

641 《International Standards on the Protection of Personal Data and Privacy》, ICDPPC,2009, Section15.1, "As a general rule, international transfers of personal data may be carried out when the State to which such data are transmitted affords, as a minimum, the level of protection provided for in this Document".

制性的隱私規則）時，仍得跨境傳輸個人資料[642]。

(三) 此外，如係為當事人於契約關係中的利益且有必要，或為保護當事人或第三人的重大利益，或為重大公共利益而基於法律要求者，均仍得依法允許跨境傳輸個人資料至未符合本標準所訂個資保護水平之國家[643]。

十四、APEC 跨境隱私保護規則體系（CBPRs）

本研究第二章第十四節提及 APEC 為促進經濟區內個人資料的自由流動，避免各會員經濟體的隱私保護規範落差形成個資跨境流通的阻礙，並同時保障個資當事人權利，特制定「跨境隱私保護規則體系（Cross Border Privacy Rules System, CBPRs）」供會員經濟體加入。

在會員經濟體加入 CBPRs 並指定當責機構 AA 做為驗證機構後，經濟體內之企業即應先符合 CBPRs「隱私框架（APEC Privacy Framework）」的規範，之後再向 AA 申請驗證。

前述 CBPRs「隱私框架」的重要原則包含[644]：

---

642 《International Standards on the Protection of Personal Data and Privacy》, ICDPPC,2009, Section15.2, "It will be possible to carry out international transfers of personal data to States that do not afford the level of protection provided for in this document where those who expect to transmit such data guarantee that the recipient will afford such level of protection; such guarantee may for example result from appropriate contractual clauses. In particular, where the transfer is carried out within corporations or multinational groups, such guarantees may be contained in internal privacy rules, compliance with which is mandatory".

643 《International Standards on the Protection of Personal Data and Privacy》, ICDPPC,2009, Section15.3, "Moreover, national legislation applicable to those who expect to transmit data may permit an international transfer of personal data to States that do not afford the level of protection provided for in this Document, where necessary and in the interest of the data subject in the framework of a contractual relationship, to protect the vital interests of the data subject or of another person, or when legally required on important public interest grounds".

644 《Updates to the APEC Privacy Framework》, APEC, 2016.

（一）避免侵害（Preventing Harm）

指企業應瞭解當事人對其隱私享有正當的期待，因此，個資保護制度的設計應致力於避免個資遭到誤用[645]。

（二）告知義務（Notice）

指個資控制者應就其對個人資料的政策對當事人提供清楚且易於取得之聲明[646]。

（三）目的限制（Collection Limitation）

指個資的蒐集須與目的相關且必要，並須以合法、公正之方式蒐集[647]。

（四）個資使用（Uses of Personal Information）

個人資料原則上僅能在蒐集目的或與蒐集目的相容（compatible）或相關（related）之範圍內使用[648]。

（五）選擇權（Choice）

在適當的情況下，個資控制者應對當事人提供清晰、明顯、易懂、易取得且可負擔的機制，供其行使與個資

---

[645] 《Updates to the APEC Privacy Framework》, APEC, 2016, para20, “Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information”.

[646] 《Updates to the APEC Privacy Framework》, APEC, 2016, para21, “Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information”.

[647] 《Updates to the APEC Privacy Framework》, APEC, 2016, para24, “The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means”.

[648] 《Updates to the APEC Privacy Framework》, APEC, 2016, para25, “Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes”.

蒐集、使用和揭露有關之權利[649]。

（六）個資完整性（Integrity of Personal Information）

個資控制者應在使用個資之目的必要範圍內，確保個人資料的正確、完整與即時[650]。

（七）安全維護（Security Safeguards）

個資控制者應以適當安全措施保護其保有之個資，以降低個資侵害風險，例如遺失或未獲授權的存取、銷毀、使用、修改、揭露或其他誤用情形[651]。

（八）存取及更正（Access and Correction）

當事人應有權「要求個資控制者告知是否保有其個資」、「要求個資控制者提供其個資」及「質疑個資的正確性，且如適當，可更正、補充、修改或刪除個資」[652]。

（九）歸責性（Accountability）

個資控制者應負責以適當措施遵循上述原則。如須

---

649 《Updates to the APEC Privacy Framework》, APEC, 2016, para26, “Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information”.

650 《Updates to the APEC Privacy Framework》, APEC, 2016, para27, “Personal information should be accurate, complete and kept up-todate to the extent necessary for the purposes of use”.

651 《Updates to the APEC Privacy Framework》, APEC, 2016, para28, “Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses”.

652 《Updates to the APEC Privacy Framework》, APEC, 2016, para29, “Individuals should be able to: a) obtain from the personal information controller confirmation of whether or not the personal informationcontroller holds personal information about them; b) have communicated to them, after having provided sufficient proof of their identity, personal information about them;…c) challenge the accuracy of personal information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted”.

將個資傳輸給第三人或組織，無論境內或境外，個資控制者均應取得當事人同意，或執行盡責調查並採取合理步驟以確保個資接受人或組織將依循上述原則保護個人資訊[653]。

又歐盟對於跨境傳輸個資的「適足性」基準之一「約束性企業規則（BCR）」之操作與 CBPRs 類似，均是由企業導入適當的管理制度以證明個資保護水平滿足規則設立的最低限度，因此 BCR 及 CBPR 之相容性即值得討論。歐盟對此曾於 2014 年發布意見[654]，特比較分析 BCR 與 CBPR 兩者對企業要求的異同，但對兩者的相容性似仍正與 APEC 努力達成共識中[655]。

此外，歐盟《個人資料保護規則》明文將「取得認證」作為具備個資保護「適足性」的判斷標準，但符合資格之標章或標準須由歐盟相關主管機關予以認許核准，因此，未來 APEC CBPRs 得否成為歐盟認許的「認證」尚有待觀察。

---

653 《Updates to the APEC Privacy Framework》, APEC, 2016, para32, "A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles".

654 《Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents》, WP212, 2014。

655 郭戎晉，《個人資料跨境傳輸之法律研究》，科技法律透析，第 27 卷第 8 期，2015 年，頁 52。

第三節　研究發現與建議（代本章結論）

一、跨境傳輸個資立法模式

在立法技術上，跨境傳輸個資之規範應可區分為「任意制」、「報備制」、「許可／同意及例外允許制」、「例外限制禁止制」等模式，以及「不區分境內外傳輸個資制」，以下僅就本研究所選國家規範方式及其優缺點整理如下：

(一) 任意制：研究對象中無國家採行

1、意義：不限制任何個資跨境傳輸。

2、優點：個人資料自由流通。

3、缺點：當事人無法獲得保障。

(二) 報備制：研究對象中無國家採行

1、 意義：向主管機關報備後即可跨境傳輸個資。

2、 優點：個人資料自由流通。

3、 缺點：當事人無法獲得足夠保障。

(三) 許可／同意及例外允許制：歐盟、英國、日本、香港、澳門、新加坡、馬來西亞、南韓

1、 意義：僅特定情形允許跨境傳輸個資，例如「主管機關許可」、「當事人同意」、「其他例外如履行契約所必須、公共利益、法律要求等」。

2、 優點：當事人獲得較佳保護。

3、缺點：阻礙個資自由流通、個資傳輸者負擔較大。

(四) 例外限制禁止制：我國、紐西蘭

1、意義：僅在特定情形限制或禁止跨境傳輸個資，例如「個資接受者所在國法規保護不足」等。

2、優點：個人資料自由流通、個資傳輸者負擔較小。

3、缺點：當事人無法獲得事前保障。

(五) 不區分境內外傳輸個資：加拿大、菲律賓

1、意義：個資蒐集機關應以相同控管方式確保境內外個資接受者保障個資之安全。

2、優點：個人資料自由流通。

3、缺點：僅由個資傳輸者對境外個資接受者控管風險。

二、跨境傳輸法制調整建議

由上研究可知，多數國家對於跨境傳輸個資係採「許可／同意及例外允許制」，一方面顧及人民的個資與隱私保護，二來尚不至嚴重影響個人資料的跨境流通，本研究從之，認為我國亦以修改為此規管方式為宜。

然而，由現實執行層面考量，如要求國家事前許可或審查例外，勢必須有足夠之人力、經費等資源支撐。是本研究建議：

(一) 如我國未來成立個資保護專責機關，由於專責機關應有適當且充足的人力、經費等資源，考量符合國際趨勢以追求對當事人足夠之保障，我國對於跨境傳輸個資之立法即應修改為

「許可／同意及例外允許制」。

(二) 若我國仍維持現狀，由各中央目的事業主管機關個別管理所轄事業的法律遵循，則仍應保留現行的「例外限制禁止制」，但應有相關配套措施以加強我國境內當事人權利之保障，例如在我國個資法第 21 條第 3 款「接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞」的限制條件下增列具體判斷依據，以供中央目的事業主管機關及個資傳輸者作為參酌。判斷依據中可包含：

1、個資接受國相關法規對於當事人權利的保護程度與我國或國際規範的差異。

2、當事人於個資接受國的救濟管道是否充足。

3、個資接受國有無個資或隱私保護的主管或監督機關，足可確保或協助當事人權利行使。

綜上，本研究參考前述國家法規，建議將個資法第 21 條修正如下：

表 4《個人資料保護法》修正草案（國際傳輸）

個人資料保護法修正草案		
修正條文	現行條文	說明
第二十一條 （甲案，如成立專責機關） **公務機關或非公務機關為國際傳輸個人資料，僅得將個人資**	第二十一條 非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事	（甲案） 我國如成立個資保護專責機關，即應將跨境傳輸個人資料之規定改採多

料傳輸至經主管機關認許具備完善之個人資料保護法規之國家。但有下列情形之一者，不在此限： **一、公務機關執行法定職務所必要。** **二、非公務機關履行法定義務所必要或協助公務機關執行法定職務所必要。** **三、當事人經告知國際傳輸個人資料之目的、類別、對象及接受國並非主管機關公告具備完善之個人資料保護法規之國家後，明示同意該國際傳輸。** **四、該國際傳輸係非公務機關為履行與當事人間之契約義務所必要，或係應當事人要求之締約前準備行為所必要。** **五、該國際傳輸係為重大公共利益所必要。** **六、該國際傳輸係為保障當事人的重大利益。** （乙案，未成立專責機關）	業主管機關得限制之：一、涉及國家重大利益。二、國際條約或協定有特別規定。三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。四、以迂迴方法向第三國（地區）傳輸個人資料規避本法。	數國家的「例外允許制」，爰參考歐盟個人資料保護規則第 45 條及第 49 條、英國個人資料保護法附表 4、日本個人情報保護法第 23 條等規定，修正本條內容。 （乙案） 若我國未成立個資保護專責機關，則仍維持現行「例外限制禁止制」，但應增列接受國個資保護法規是否完善的具體判斷依據，以供中央目的事業主管機關及個資傳輸者作為參酌，爰參考加拿大個資保護及電子文件法附表 1 第 4.1.3 條及紐西蘭隱私法第 114B 條等規定，修正本條內容。

非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：一、涉及國家重大利益。二、國際條約或協定有特別規定。三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。 四、以迂迴方法向第三國（地區）傳輸個人資料規避本法。 **中央目的事業主管機關於依考量前項第三款接受國對於個人資料之保護是否具有完善之法規時，應審酌下列事項：一、接受國相關法規對於當事人權利的保護程度與我國或國際規範的差異。二、當事人於接受國的救濟管道是否充足。三、接受國有無個資或隱私保護的主管機關，足可確保或協助當事人權利行使。**		
第四十七條 （甲案，如成立專責機關） 非公務機關有下列情事之一者，由**主管機關**處新臺幣五萬	第四十七條 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、	配合我國成立個資保護專責機關與否之修正。

元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之：一、違反第六條第一項規定。二、違反第十九條規定。三、違反第二十條第一項規定。四、**違反第二十一條規定**。 （乙案，未成立專責機關） 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）政府處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之：一、違反第六條第一項規定。二、違反第十九條規定。三、違反第二十條第一項規定。四、違反中央目的事業主管機關依第二十一條**第一項**規定限制國際傳輸之命令或處分。	縣（市）政府處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未 改正者，按次處罰之：一、違反第六條第一項規定。二、違反第十九條規定。三、違反第二十條第一項規定。四、違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或處分。	

第四章 結論

本研究聚焦於「個資與隱私保護專責機關」與「個人資料跨境傳輸與資料在地化」的國際實踐，於比較國際法例、規範後產出研究發現，並依此提出我國的修法建議。

在「**個資與隱私保護專責機關**」部分，本研究於第二章提出下列發現與建議：

一、 研究國家均設有獨立個資保護專責機關

包含歐盟(各會員國)、英國資訊委員辦公室、加拿大隱私委員辦公室、香港個人資料私隱專員公署、澳門個人資料保護辦公室、日本個人情報保護委員會、南韓個人資訊保護委員會、新加坡個人資料保護委員會、菲律賓國家隱私委員會、馬來西亞個人資料保護署、紐西蘭隱私委員辦公室及澳洲資訊委員辦公室。

上述機關均係該國法律明定的個資或隱私保護法律主管機關，其法定任務即為監管個資或隱私保護法律，因此具有足夠的「專責性」，足以其人力、經費、設備等資源實際執行個資或隱私保護法律的法定職權。

二、 專責機關須具備獨立性

除前述「專責性」外，個資保護專責機關尚須具備足夠之「獨立性」，以確保能客觀、公正執行職務，歐盟更於相關法律條文中要求此獨立性為「完全之獨立性」，其內涵亦經歐洲法院於司法判決中反覆重申係指「機關不得存有直接或間接受到任何來自外部之影響，致其決定有偏頗之虞的可能」。

因此，獨立性要求不僅體現於專責機關「功能」層面，亦

延及專責機關的「組織」、「人事」及「財務」之獨立。在此條件下，歐盟對專責機關的獨立性要求，幾近我國《中央行政機關組織基準法》規定的「獨立機關」。

三、 專責機關須有足夠的法定任務與職權

此外，專責機關尚需有足夠的「法定任務」，方可落實個資與隱私保護，又為達成法律賦予之任務，專責機關亦需有足夠的「法定職權」才能有效執行。

本研究發現，歐盟依法授予專責機關的法定職務可區分為「指導」、「核准」、「執法」與「申訴處理」四大類，其他國家的專責機關法定職務亦可歸納至此四大類中開展。

相較之下，我國個資法雖賦予中央目的事業主管機關「執法」權力，但在「指導」任務部分卻較國外法例不足，使得我國公務機關及非公務機關僅能依法務部及中央目的事業主管機關的「被動解釋」，於個案摸索、拼湊個資法的全貌。

另雖在現行個資法規範下，當事人如認其個人資料遭受不法侵害，應可向對其侵害之非公務機關的中央目的事業主管機關申訴請求為必要行為，然參酌外國法例，當事人申訴的權利、條件、程序及受理機關處理案件的條件、程序等事項，仍應有法律或法律授權之命令明定為宜。況如人民對於「公務機關」違法致其個人資料遭不法侵害時，除循民事程序求償（但人民對於公務機關違法事實之舉證常因資訊不對等而不足）外，似無一明確可協助人民調查事件、釐清事實的外部公權力機關供人民申訴。

據此，如我國成立具備足夠資源的個資保護專責機關，即可參酌外國法例，於個資法「個人資料保護法修正草案」中增

訂「當事人向主管機關對公務機關或非公務機關提出申訴」之相關規定，及「主管機關得主動或經當事人依法申訴而對公務機關發起調查或對非公務機關進行行政檢查之權力」等文字。

四、 我國成立個資保護專責機關之困境及法規調適建議

綜上，本研究於第二章整理各國家及國際組織對於個資與隱私保護專責機關的組織要求(專責性與獨立性)與法定職務，並提出「各國個資與隱私保護專責機關彙整表」、「歐盟個資保護監督機關任務與職權分類表」及「各國個資保護專責機關重要職務對照表」。

基於上述研究發現與 vTaiwan 線上徵詢之公眾意見，成立個資專責機關似為國際趨勢，除可統一解釋個資法並於個案中認定事實涵攝之外，亦可發揮「事前指導」功能，協助並輔導我國公務機關與非公務機關妥善遵循與因應法律規範，並能有一致性的標準執行行政檢查與行政處罰。

惟我國目前如欲成立個資專責機關，受有相關限制：如欲以二級或三級中央行政機關方式設立，按現行《中央行政機關組織基準法》規定，已達機關數量上限，無法新設行政機關;縱可修法新設行政機關，因我國行政機關受行政一體監督，首長不享任期保障，於人事及功能上，是否可發揮獨立性，尚有疑慮。如欲保有個資專責機關之獨立性，擬以獨立機關方式設立，按現行《中央行政機關組織基準法》第 32 條第 2 項規定，我國相當二級機關之獨立機關組織，已達數量上限，無法新設獨立機關；相當中央三級機關之獨立機關組織，或有設立空間，惟三級獨立機關是否可發揮協調之有效性，亦有疑慮。

未來如政策規劃成立個資專責機關，建議修正《中央機關組

織基準法》有關組織規模之建制標準外，另依「中央機關組織基準法」第 5 條第 3 項原則不得以作用法規定機關之組織之規定，因目前個資法性質為作用法，併建議配套訂定個資專責機關之組織依據。

而在「**個人資料跨境傳輸與資料在地化**」方面，本研究於第三章整理各國家及國際組織對於個人資料的跨境傳輸與資料在地化規範，認為我國不宜採行嚴格的「資料在地化政策」，而應維持「有條件的跨境傳輸」立法模式。

在研究**對象**中，多數國家（歐盟、英國、日本、香港、澳門、新加坡、馬來西亞、南韓）對個人資料的跨境傳輸係採「許可／同意及例外允許制」，與我國個資法第 21 條的「例外限制禁止制」相異。

本研究認為，由政府主動把關個人資料的安全與當事人權利之保障，方足落實國家保護人民權利不受侵害之義務，因此，建議我國仿效多數國家對於跨境傳輸個人資料所採的「例外始允許」之規管模式。然在現實考量下，審查跨境傳輸個人資料是否符合例外，需有足夠人力、經費作為支援，在現行個資法由各中央目的事業主管機關分別管理所轄事業的情況下，難以期待各主管機關撥出足夠資源以執行審查，況分由不同主管機關審查跨境傳輸的許可，將可能導致同一或類似事件而有不同認定之歧異，對我國個資保護的實踐亦非善事。

因此，本研究建議，如配合個人資料保護委員會之成立，我國個資法第 21 條關於「國際傳輸個人資料」之規範即可一併修正，改為「許可／同意，例外允許制」，以強化電子商務、社群網路時代的國民個資與隱私保護；若我國未能成立個資保護

專責機關，則仍應維持現行「例外限制禁止制」，但對於中央目的事業主管機關在「審酌個人資料接受國對於個資保護是否具備完善之法規」時，應有法定標準以憑依據。

本研究據此於第三章第三節提出《個人資料保護法》修正草案，並以甲乙兩案呈現「成立個資保護專責機關與否」對應的個資法第 21 條有關「國際傳輸個人資料」修正內容，供委託機關參考。

第五章 參考資料

中文資料

1、 專書

（1）原著:(德)Chrstopher Kuner,譯者:旷野、杨会永等(2008)，*欧洲数据保护法：公司遵守与管制*，中國法律出版社。

（2）呂錦峰、謝持恆（2012），*個人資料保護法教戰守則*，永然文化出版股份有限公司。

（3）劉佐國、李世德（2012），*個人資料保護法釋義與實務—如何面臨個資保護的新時代*，碁峰資訊股份有限公司。

（4）蕭家捷、賴文智（2013），*個人資料保護法 Q&A*，元照出版有限公司。

2、 論文

（1）林詩韻（2012 年 1 月），*銀行國際傳輸客戶資料保護規範—以英國法為中心*，國立政治大學法學院碩士在職專班碩士論文。

（2）黃莉雲（1994），*資料跨國流通法律問題之研究—相關理論與規範*，國立臺灣大學法律學研究所碩士論文。

（3）翁逸泓（2005 年 12 月），*歐洲個人資料保護之研究—以歐洲經驗反思我國作為*，南華大學歐洲研究所碩士論文。

3、 期刊

（1）周慧蓮(2004)，*資訊隱私保護爭議之國際化*，月旦法學雜誌，

第 104 期，頁 112-132。

（2）郭戎晉（2015），*個人資料跨境傳輸之法律研究*，科技法律透析，第 27 卷第 8 期，頁 28-55。

（3）洪榮彬(1995)，*論資訊時代跨越國境之資料處理與資料保護*，法學叢刊，第 199507（40：3）期，頁 80-103。

（4）翁清坤（2010），*論個人資料保護標準之全球化*，東吳法律學報，第 22 卷第 1 期，頁 1-60。

（5）陳榮傳（2001），*再論資料跨國流通*，月旦法學雜誌，第 78 期，頁 165-177。

（6）鄭美華（2017），*數位經濟時代下的非關稅障礙？—淺談全球「資料在地化」政策及法制的興起*，NCC NEWS，第 10 卷第 11 期，頁 21-27。

（7）鄭美華(2017)，*歐盟個人資料保護規則之淺介*，NCC NEWS，第 11 卷第 6 期，頁 9-12。

4、研究報告

（1）余啟民、吳君婷、王慕民、陳品安、吳彥欽、張又丹（2016），*通訊傳播事業個人資料保護之機制及管理模式委託研究報告*，國家通訊傳播委員會委託研究報告。

（2）林秀蓮、李世德（2014），*考察南韓、新加坡個人資料保護法制及相關專責機關*，法務部出國考察報告。

（3）范姜真媺、劉定基、李寧修（2016），*歐盟及日本個人資料保護立法最新發展之分析報告*，法務部委託研究報告。

（4）范姜真嫩、高啟中、翁清坤、李寧修（2015），*我國電信業及電信加值網路業個人資料保護與監管機制之研究*，國家發展委員會委託研究報告。

（5）陳維練、鍾瑞蘭、李世德、林辰芸（2013），*考察澳門、香港「個人資料保護專責機關」報告*，法務部出國考察報告。

外文資料

1、 司法判決

（1）European Court of Justice, Case C-518/07, Commission v. Germany, 2010。

（2）European Court of Justice, Case C-614/10, Commission v. Austria, 2012。

（3）European Court of Justice, Case C-288/12, Commission v. Hungary, 2014。

2、 研究報告

（1）Centre for Information Policy Leadership at Hunton & Williams LLP（2017），*Regulating for Results: Strategies and Priorities for Leadership and Engagement discussion paper*。

（2）Information Technology Industry Council（2017），*Data Localization Snapshot*。

3、 實務指引與工作文件

（1）加拿大（2009），*Processing Personal Data Across Borders*

Guidelines。

（2）歐盟（1998），T*ransfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive*，WP12。

（3）歐盟（2002），*Opinion 4/2002 on the level of protection of personal data in Argentina*，WP63。

（4）歐盟（2003），*Opinion 5/2003 on the level of protection of personal data in Guernsey*》，WP79。

（5）歐盟（2004），*The application of Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland*。

（6）歐盟（2006），*The application of Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documentation Act*。

（7）歐盟（2007），*Opinion 8/2007 on the level of protection of personal data in Jersey*，WP141。

（8）歐盟（2007），*Opinion 9/2007 on the level of protection of personal data in the Faroe Islands*， WP142。

（9）歐盟（2009），*Opinion 6/2009 on the level of protection of personal data in Israel*，WP165。

（10）歐盟（2009），*Opinion 7/2009 on the level of protection of personal data in the Principality of Andorra*，WP166。

（11）歐盟（2010），*Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay*，WP177。

（12）歐盟（2011），*Opinion 11/2011 on the level of protection of personal data in New Zealand*，WP182。

官方網站

1、英國 ICO：https://ico.org.uk/

2、加拿大 OPC：https://www.priv.gc.ca/en/

3、香港個人資料私隱專員公署：https://www.pcpd.org.hk/cindex.html

4、澳門個人資料保護辦公室：http://www.gpdp.gov.mo/

5、日本個人資訊保護委員會：https://www.ppc.go.jp/en/

6、新加坡 PDPC：https://www.pdpc.gov.sg/

7、南韓 PIPC：http://www.pipc.go.kr/cmt/main/english.do

8、馬來西亞 JPDP：http://www.pdp.gov.my/index.php/en/

9、菲律賓 NPC：https://privacy.gov.ph/

10、紐西蘭 OPC：https://privacy.org.nz/

11、澳洲 OAIC：https://www.oaic.gov.au/

各國法例

1、 歐盟：《General Data Protection Regulation》

2、 英國：《Data Protection Act》

3、 加拿大：《Privacy Act》,《Personal Information Protection and Electronic Documents Act》

4、 香港：《個人資料（私隱）條例》

5、 澳門：《個人資料保護法》

6、 日本：《個人情報の保護に関する法律》

7、 南韓：《Personal Information Protection Act》

8、 新加坡：《Personal Data Protection Act》

9、 馬來西亞：《Personal Data Protection Act》

10、菲律賓：《Data Privacy Act》

11、紐西蘭：《Privacy Act》

12、澳洲：《Privacy Act》、《Australian Information Commissioner Act》

13、中國：《網絡安全法》

14、俄羅斯：《資料在地化法（Data Localization Law）》

15、印度：《國家資料分享及存取政策（National Data Sharing and Accessibility Policy）》

16、印尼:《資訊及電子交易法（Information and Electronic Transaction Law）》

國際組織規範

1、ICDPPC：《International Conference of Data Protection and Privacy Commissioners RULES AND PROCEDURES》, 2017

2、ICDPPC：《Counting on Commissioners：High level results of the ICDPPC Census 2017》, 2017

3、APEC ：《 APEC COOPERATION ARRANGEMENT FOR CROSS-BORDER PRIVACY ENFORCEMENT》, 2009

4、APEC：《Updates to the APEC Privacy Framework》, 2016

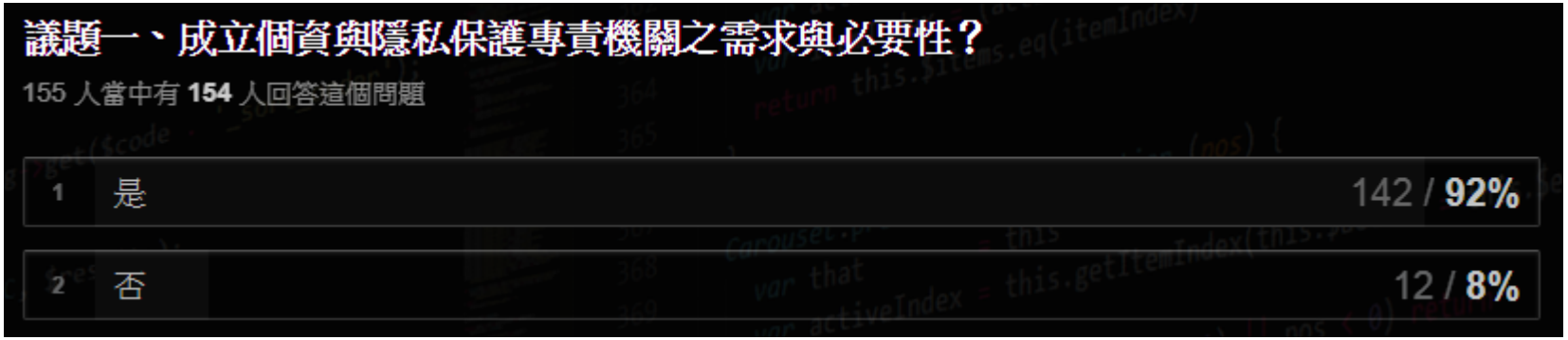
5、OECD：《 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data》,2013

附件：vTaiwan 個資與隱私保護專責機關線上意見徵集彙整（2017/11/08-2017/12/31）

註 1：線上公開問卷彙整結果之連結（僅公開封閉性問答之部分）：https://audreyt.typeform.com/report/zeFg10/cGOsa6E8liCRXW35

註 2：其他有關推薦人選、是否公開意見、填答人之個人資料與問卷意見回饋，請參照 Excel 檔

議題一、成立個資與隱私保護專責機關之需求與必要性？



您選擇有必要的理由是？（可略）

統一性

- 如能有個資保護專責機關，可以統一各機關保護個人資料的見解

- 統一解釋法令 符合國際規範
- 解釋個資及隱私可以統一解釋
- 由一個機關統一見解，在依各事業所發生之個資議題函詢各主管機關，可避免現行法務部解釋個資法，各主管機再視情形修正之狀況
- 統一法令解釋，避免在不同的主管機關的解釋相互衝突，增加法規的透明度
- 避免解釋歧異，造成法規適用之混亂
- 事權統一，部會間不會互推
- 執行標準不一，統整與其他組織或國家在個資交換處理上的差異
- 統一執法標準，較不會有某些主管機關或對某些行業較積極監督管理，其餘則較鬆散的情形
- 統一解釋個資相關疑義，並提供各法院法官判決依據
- 許多隱私問題不能等待法院作成判決之後才能明確。獨立機關可提供事先的規則供機關遵循，而且可避免由各中央部會主管機關解釋時，球員兼裁判的問題
- 無論政府、教育或民間對個資法都有自己的解讀，無法有效利用和保護個資，失去立法原意
- 在不同機關單位之間需要統一控管隱私洩漏多寡

- 個資法通過後，許多機關或企業已開始有基本保護個資意識。如同本提案宗旨『有所出入』，本人以個人經驗為例分享，眾多單位皆會以星號＊做為遮蔽，然而因沒有統一規範，各單位遮蔽位置不一。實務上一個人手中所持有文件絕非一份，眾多文件組合下，星號並無具體效用
- 個資保護橫跨各目的事業，需統一解釋及適用
- 由專責機關統一處理個資事項可免除多頭馬車或見解不一的狀況
- 統一解釋法規及問題，避免機關彼此卸責
- 目前散落在各目的事業主管機關管轄下，每個目的事業主管機關之認定與判斷標準恐有差異

專責性

- 為了讓個資與隱私保護有專責的單位能負責而不是分散在各單位
- 釋法的專業能力
- 權責分明
- 保護個人資料，同時也要兼顧研究發展，需要一個專門處裡的機關單位
- 當今數位資訊時代，個人及隱私資訊往往被要求於多個公司或機關。若無善盡管理責任，易造成大眾財物損失抑或是權利受損未來，物聯網、車聯網時代，多筆資料將以訊號流竄於城市間，有心人士若掌握這些資料可能將損及民眾之權益或財物

- 避免各個單位都管，結果最後沒有人管
- 法律專業、技術專業(資安設備)、對各行各業(業務)特性之專業度
- 現今尚未有單位能獨立作業相關管理，且執行需要相關專業知識，能由專門單位負責較佳
- 事權統一。連垃圾廢棄物事宜都有中央專責機關(環保署)及地方專責機關(環保局)，難道個人資料保護不如垃圾
- 確實導致執法不彰無法使違法者受罰之情形
- 因為各單位解讀不一會造成社會與企業無所是從。而且對當事人的權益主張也較不利。歐盟 GDPR 也是採用專責單位的設計
- 如果沒有的話，無法與國際組織有所合作
- 以使個人資料處理更專業
- 要有獨立性
- 權責清楚，利於規範
- 因為這也是一種專業，更是當前最重要的事情之一
- 隱私權是憲法保障人民的基本權利，應由一獨立機關來保護
- 避免政治勢力介入造成人民個人資訊被公開

- 要有位階明確且足夠的機關踐行各資法的保障跟監督
- 有專責監督機關能更加確保個資法之執行有所保障
- 因應科技和資訊發展，未來相關的問題可能會越來越多（尤其是生醫產業），現行的問題是主管機關權責不足，以及一般民眾缺乏相關認知，建議可以建立專責機關，進行統一解釋、宣導、教育等工作
- 個人資料保護應免於政治、公益團體的介入方能贏得人民的信任，有詐騙集團猖獗可見個人資料保護已刻不容緩
- 相關議題可能引起爭論，如果有主管機關負責，才能夠制定合理的標準，做出合理的保護，但不過度限制
- 有專責機關統一解釋，並監督管理
- 現行各部會對於個資標準標準不一，實際上法務部並無各部會之能力，往往為了特定政治、經濟、租稅等目的，使個資法之淪為具文，有必要成立專責機構
- 數據會是未來的重要資源 但是怎麼使用如何管理 不管是針對興利或防弊都需要專責研討
- 成立隱私專責機關當然是國際潮流，但絕不只是國際潮流的問題而已。台灣目前的《個人資料法保護》是交由各目的事業主管機關去落實，法務部則為解釋機關，這樣的分工不僅容易使《個資法》法律解釋的公正性遭人質疑外，也會使人民的隱私受到各部會標準不一的保護。且更會因各部會的主要職掌並非隱私保護，以及隱私權傷害幽微不易察覺的特性，使其容易淪為該部會在落實其主要業務時首要犧牲的權利。　在數位時代，資料的蒐集、處理、利用方式因科技進步與被大幅利用，已與行政機關的業務或市場經濟的發展再也分不開，也因

此稍有不慎，這樣的結合可能會使政府擁有過大權力行國家監控或對不同族群的人民行差別待遇，或使商業公司得以任意操弄消費者的偏好或情緒以改變其生活處境或判斷等。類似的案例世上舉目皆是。當一個國家缺乏隱私專責機關，沒有人可以去客觀衡量公、私部門的政策或營業模式對隱私保護的衝擊，人民若要得以保有一個基本自由養成的空間，可能只能倚賴運氣與福份

- 專責機構可專門處理這類型的案件糾紛，有迅速、專業的優點

隱私與個資保護的重要

- 隱私侵害的隱微性
- 保護人民隱私
- 個人隱私是一個個人的權利，不需要的時候就不需要，需要的時候很重要
- 維護個人隱私
- 個資意識提升，且個資法通過後人民將依個資法行使其權力。當行使活動增加時，相關衍生問題有可能伴隨發生，因此設立專責機關有其必須性
- 個人資料屬於隱私，不應出現在公領域的場合，需有良好的保護機制。在網路時代，個人資料也可作為各種商務交易，若未能良好管理，也將放縱網路犯罪。
- 隱私很重要阿

- 保護個資
- 保護個資
- 隱私
- 現行個資隱私資料外洩事件頻傳，易遭有心人士利用於詐騙或其他不法行為
- 隱私權是憲法所保障的權利，政府有義務保護人民的隱私
- 個資很重要
- 我的資料為什麼不該被保護　　世界上那麼多國家都有做到保護人民　我們隨隨便便都可以肉搜人出來被公審被私刑　人們都會接到莫名其妙的詐騙電話這難道不該視為人民的個人資料不斷被洩漏嗎 這樣的社會真的安全嗎
- 個人資料需要被保護
- 個人資料的保護，乃是現代科技進步下，政府應多加注意的事項！且為了與歐盟談判，請正式此議題
- 隱私權已經是國際都很注重的，如果要跟國際平起平坐，我們的個人資料保護就要做的更好
- 個人資料很重要
- 網路現今越來越發達，不管是網路購物還是線上申辦帳號等等，因此個資的問題也變得更重要，再加上最近也

出現許多利用其他工具代替現今支付，所以個資遠比想像中更重要。

- 隱私權必須受保障
- 隱私權應該被重視
- 隱私這部份好像沒有很受保護
- 隱私權
- 每個人對於自己的基本資料本來就有保護 被保護的權利
- 在台灣取得個人資料太容易
- 網路個資太容易外漏
- 台灣的個資容易外流
- 台灣企業個資外洩狀況浮濫，目的事業主管機關幾無作為，放任包庇業者侵害消費者資訊隱私權，造就台灣一直無法有效處理的詐騙問題，年年衍生龐大司法處理成本，在首腦多在海外抓不到的狀況下，政府又不就源頭去管制，就是包庇。
- 因為我個資外洩被詐騙，正在打官司中
- 台灣許多網購、電商業者有個資外洩的情形

- 「EZ 訂」個資嚴重外洩,請問有人知道如何求償嗎？ 希望可以找出共同受害者,一起維護個人的個資法權益。政府單位推個資法，卻一直允許讓企業個資不斷外洩，真正的受害老百姓，卻無處申冤...
- 台灣電商個資外洩太嚴重了
- 個資是對於台灣發展的關鍵議題，若不做適當管理而一昧禁止，對台灣不利
- 網路太發達，個人資料很容易外洩
- 國家對於私人資訊有更長遠的想法與預測
- 人民的個人資料有權不受他人窺探的權利
- 落實人權的保障，避免個資流落至有心人士

國際接軌

- 才能與國際接軌
- 與國際接軌，與我國與他國之資料相互傳輸以及保護
- 才可與國際接軌，使得我們的個資才可以在國際傳輸不受阻礙

其他

- 非常必要！
- 擬定保護等級並針對需求給予證書, 查驗保護等級並依法監督或進行查驗
- 依法行政
- 我國政府現下並不重視這些重要法案的推動，需要更多的人關注
- 減少電話詐騙和騷擾
- 資訊爆炸年代這樣的機關是必要的
- 人民要有知的權利
- 保護人民權利
- 很重要
- 基本人權之一
- 防止詐騙

您選擇沒有必要的理由是？（可略）

- 個資使用遍佈甚廣，單一可能會發生責任全扛但任務都沒有辦法做

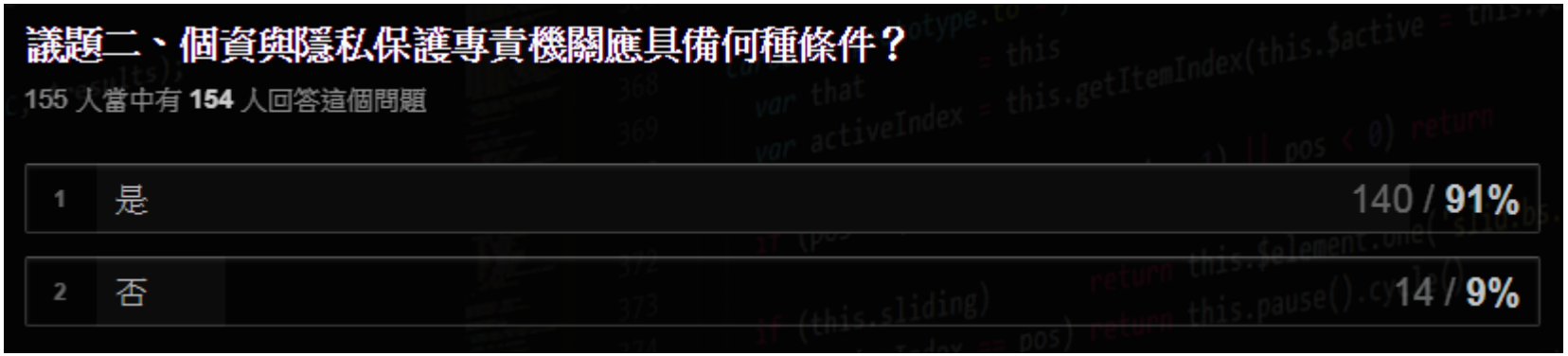
- 因為只要做好 security and privacy 的規定由現有單位執行監督既可
- 現有體制下，機關過多，容易造成疊床架屋。改由司法院所屬分派出一個單位執行
- 與現有機制重複、疊床架屋
- 成立辦公室，下面沒有了，法務部當負起國家法制調適的責任

議題二、個資與隱私保護專責機關應具備何種條件？

參照世界各國之個資與隱私保護專責機關均具有專責性，惟獨立性的內涵不盡相同，如我國未來成立個資與隱私保護專責機關，除具備專責性之外，是否須具備獨立性之要件？

獨立性：依據法律獨立行使職權，自主運作，除法律另有規定外，不受其他機關指揮監督。

【如果我國成立了個資與隱私保護的專責機關，您覺得它必須是獨立的嗎？】



您覺得一個理想中的個資與隱私保護機關是什麼樣子的呢？（如條件、功能……）（可略）

獨立性

- 對於保護個人資料與社會利益，必須要獨立於行政難易度與權力之外
- 獨立機關，準司法性
- 獨立機關
- 不受他人指示，人事獨立(避免現行許多機關採用官派，導致被官派人無具備該機構相關經驗，而影響機關執行成效)
- 不受行政機關的掌控（權力分立）

- 獨立性
- 合議制機關，並公正獨立
- 合議制機關，獨立於行政院之外
- 需獨立於行政院以外
- 依法獨立行使職權，不受其他機關還有政治力量干預
- 獨立行使職權，不受政治干預
- 政治中立
- 它應至少在人事、財務上要有充分資源，並具人事、財務上的獨立性。資源充份能確保其有效行使職權，而非僅是空殼組織。獨立的人事意味著其人事任命原則上應僅受該機關主管或國會的指揮，並且該機關應可選擇自身的員工，而除非有重大原因，否則無論委員或員工都不應受其他上級行政機關的指揮甚至更換；同理，財務的獨立也保證其多數時刻不受上級機關支配。如此，方有可能有效行使職權，並在職權行使上具真正的獨立性。至於功能，隱私專責機構應有接受申訴的功能；此外，它也應具備一定程度的調查權與糾正權，以及在適當時刻開啟司法程序的權限，以維持其積極保護隱私的能力。它應能在特定時刻，去要求受檢查的一方出示其如何管理個人資料的資訊，或是在確認有違反法律的情形時，命令受檢查方改善（具體如何運作可再討論）。如此方能落實個資法上的規定。它也應要能去實際參與其他機關的政策制定，就可能造成的隱私風險提出有效的建

議或評估。　此外，它也應設法提升民眾的隱私意識，使人民了解自身有何權利可主張，又要如何行使。以及因應科技發展，在現代社會生活時，其權利何時可能受到限制，或甚至受到不當侵害

- 做好解釋適用和畫好低標，給予個別領域自治空間
- 是獨立機關，合議制，該機關之處分相當於訴願決定，可直接提行政訴訟
- 獨立於政府機關部門外的委員會議性質

專業性

- 需有專業的法律，資訊工程等知識與技能
- 同第 2 題，需要有法律專業、技術專業(資安設備)、對各行各業(業務)特性之專業度
- 要懂法律更必須懂技術，現在很多個資外洩都與技術有關係，不懂技術的主管機關，如何合理判斷使用者已經善盡個資保管之責？
- 組成多元及專業
- 電腦及網路安全檢查能力, 或能進行滲透測試
- 資訊管理人員
- 需要對於相關的國際規範及其執行方式有一定程度的了解與施行能力

- 若獨立性導致該機關設立有高度困難，應先求有(專責性)，是否再求好(獨立性)，下一階段再說，先有專責機關吧，不用一步到位，否則此議題討論，永遠呈現空轉現象，無法誕生個資保護機關。至於其他條件尚須第三、分工性(橫向與中央目的事業主管機關分工模式建立，縱向與地方政府分工模式建立，不是全部由中央個資專責機關來做)。第四、國際性，單一專責機關更方便加入個人資料保護國際組織，始有辦法處理跨境個資保護議題(例如以下國際組織尚不要求到獨立性:APEC CBPRs、亞太區私隱機構組織 APPA，尤其 APPA 入會資格只要是 APEC CBPRs 會員即可加入，一魚兩吃，參考 http://www.appaforum.org/about/)。
- 最大的問題不是獨立機關跟權力，而是知識跟人手不足。
- 需要有資訊專業人員與法律專業人員
- 相關專業人士
- 個人資料防護是 IT 技術密集之工作，「十年磨一劍」， 歐盟於人才培訓已歷 10 年，GDPR 公布後尚有 2 年之準備期，美國則進行 10 年(FY2011~2020)的實作試點(1 計畫 1~2 年，政府補助約 US$2,000.000)；舉例而言，「被遺忘權」之實作技術，美國及歐盟均有行政罰則且 ISO 已有其技術標準並納入 ISO/IEC 27002/27018 等之技術控制，於我國至今幾無人實作之；淺見，宜參照歐盟或美國「技術先行」的策略，俾此「個資與隱私保護機關」具備應有之 IT 技能知識，方不重蹈將「網路實名制」之技術控制標準(CNS(ISO/IEC)29191)誤為「資料去識別化」驗證標準之覆轍。
- 能解釋實務問題，不只是法條。具法律，資訊，管理等背景之人才

- 捍衛隱私權其實亦屬於捍衛人格權，不應該以國家高權、媒體炒作煽腥的角度任意踐踏，因此專家、學者之參與組成有其必要性
- 公開性, 專業程度
- 專業性，了解數據經濟對於大公司到個人，對於國家或個體的想像與影響
- 結合各領域專家合作執行。

多元性

- 多元利害相關方
- 能以多重角度，看待個資議題

其他

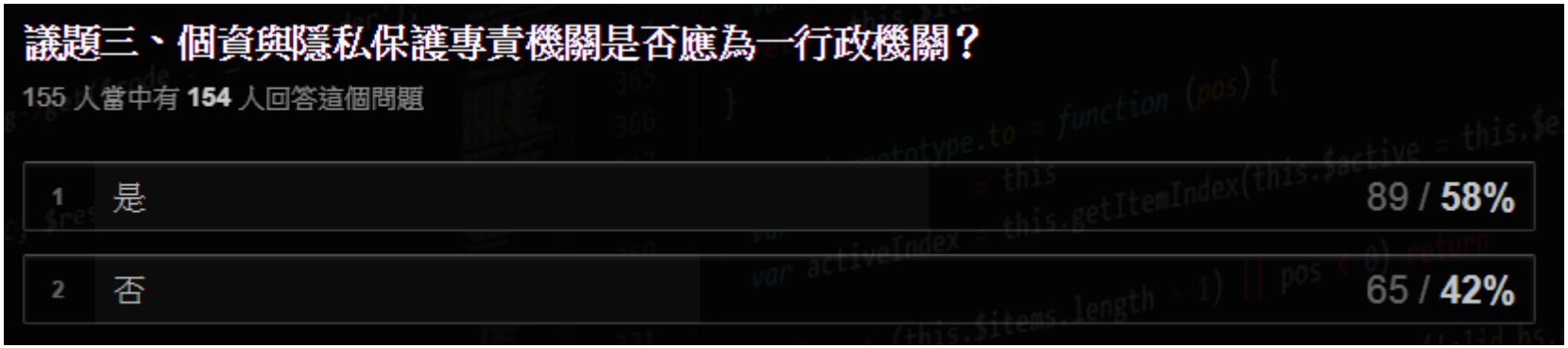
- 要能指揮及監督公務機關和非公務機關
- 如果可以適度與電信單位及司法單位合作那就更好了
- 這政府因應議題已經夠多「組織」了
- 保有產業意識，但具備高度人權自決，高度資訊安全

- 無
- 對新科技、新商業模式的適應力及彈性
- 讓民眾申訴
- 不同場域需要的資訊量與保密性不一，應該是資訊保密程度差異的問題
- 必須了解個資與應用間之平衡，不可僅偏個資保護
- 個資管理需要專責，但建議應在資安的大架構下建立
- 要有解釋權力，釋疑，並能透明開放與民眾溝通
- 足夠資源
- 中立、廉潔、知法、守法
- 民間委員過半
- 可以保護與仲裁，行政處份
- 溝通協調性：與各部會溝通協調各部會應負之責任
- 具保護性

- 需為和議制度
- 法律授權明確性
- 具有執法的能力。包括受理民眾申訴，以及調查違規案件的權力。
- 公正性
- 必須要有一定的地位，不然意見容易被其他機關吃掉
- 教育性、公益性
- 衛福部即可
- 強制力，能夠介入案件監督個資事宜
- 組織層級不宜太低
- 透明：將「資訊公開」納入成立的核心原因，務必力求公正、公開
- 要有標準作業流程，與警政單位合作，當刑事局高風險賣場報案紀錄在短時間內出現累積一定數量受害者的電商（例如 1 個月內累積 200 人報案），這個機關要主動介入，積極監督、開罰該業者改善資安，而不是放任 ez 訂這種爛業者，持續個資外洩一整年。
- 主動性：若有企業有個資外洩的嫌疑，且民眾有反應，應該要去調查

- 要提供民眾檢舉，還要有申訴管道，政府推個資法，卻讓公家機關，企業，電商，個資不斷外洩，老百姓求助無門，無處可申
- 可以隨時能督導或是監控台灣電商個資外洩的情形
- 必須具足夠公權力行使個資法所賦予之權限
- 政府機關，各縣市也有配置次級單位

議題三、個資與隱私保護專責機關是否應為一行政機關？

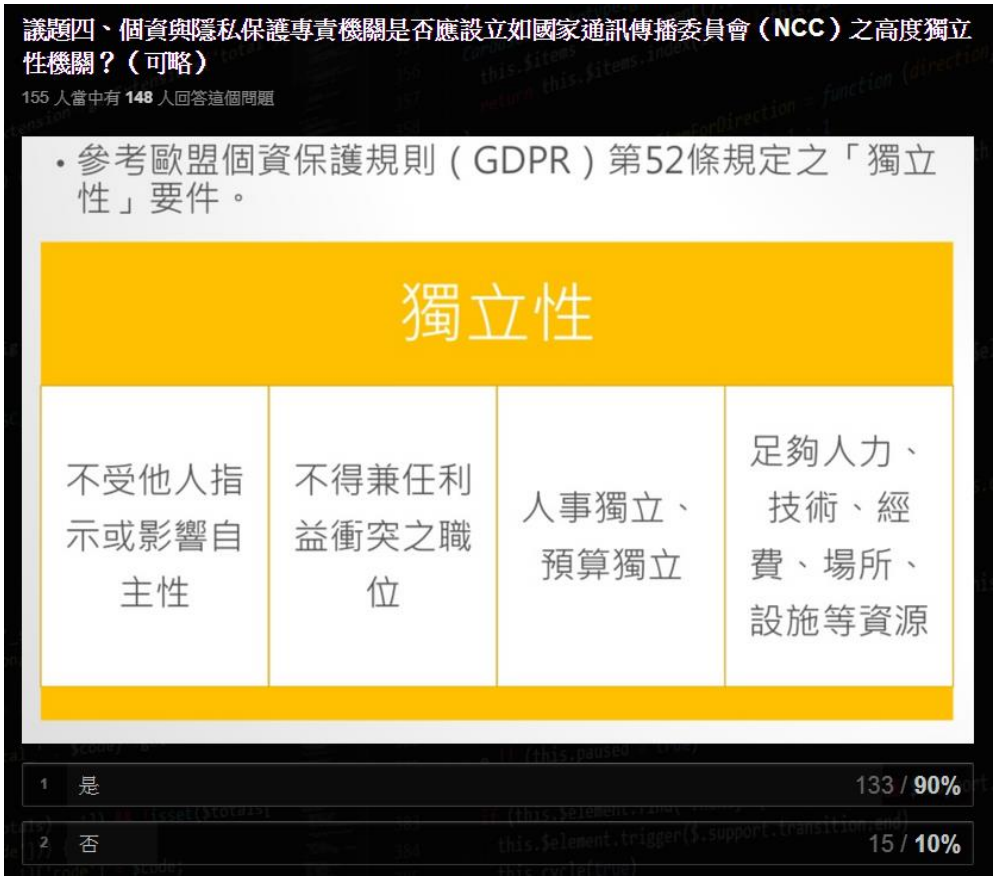


承上題，其監督管理之範圍為何？

其監督管理之範圍除了非公務機關之外，是否應包含公務機關？

【理想中的個資與隱私權保護專責機關，除了監督民間企業外，也可以監督其他的公務機關嗎？】

議題四、個資與隱私保護專責機關是否應設立如國家通訊傳播委員會（NCC）之高度獨立性機關？（可略）



請勾選您認為理想中的個資與隱私權保護專責機關應具備的獨立性要素（可複選）

議題五、如成立個資與隱私保護專責機關，應為何層級之機關？

議題六、您認為個資專責機關是否應該民間委員過半？