防貪指引-個資與保密篇

態樣 1：洩漏投標廠商家數及名稱

案情概述：

甲為某鄉公所技佐，負責該公所各項交辦工程、村里小型工程等工作，為依法令服務於地方自治團體所屬機關而具有法定職務權限之公務員，甲辦理工程採購招標時，明知開標前應依政府採購法規定保密相關資訊，竟仍基於公務員洩漏國防以外秘密之犯意，將「投標廠商家數」或「投標廠商名稱」等資訊告知廠商。

風險評估：

一、 法治觀念欠佳：

採購業務承辦人對於法令規定應保密事項，應有清楚之認知，除廠商投標文件及底價應保密外，開標前投標廠商名稱及家數等資訊，均應依政府採購法第 34 條規定予以保密。

二、 缺乏保密認知：

採購人員除知悉政府採購法應保密規定外，並應有保密之認知，且對於洩漏應保密資訊後，可能將承擔相關刑事責任有明確之認識，若因與廠商私交，而洩漏應保密資訊，將使民眾喪失對公務員執行公權力之信任。

三、 未遵守「採購人員倫理準則」：

採購人員應廉潔自持，重視榮譽，言詞謹慎，行為端莊。採購人員應遵守採購人員倫理準則，保持與廠商

之間應有之距離與分際，不得洩漏應保守秘密之採購資訊。

防治措施：

一、 強化政府採購法知能：

政府採購法訂有相關之保密規範，包含對於招標文件、底價、領標、投標廠商名稱及家數、廠商投標文件、評選委員名單等，均屬刑法所指「中華民國國防以外應秘密」之資訊，辦理採購之相關人員，均應知悉並遵守相關規範。

二、 落實平時考核：

各單位主管除應落實平時考核工作外，密切注意所屬同仁與廠商有無不當交往、接受飲宴、招待或其他不合常理的密切往來，遵守「採購人員倫理準則」及「公務員廉政倫理規範」，必要時應調整相關職務。

三、 建立多層次督導機制：

透過數個管理層級的層層把關，全面降低貪腐與舞弊的風險，確保組織的誠信與法令遵循。例如「內部控制」與「三道防線」概念，也就是透過多個層級（如第一線自查、中階主管複核、高階或獨立單位審查）的參與，達到權力制衡，防止濫用職權。

四、 辦理公務機密檢查作業：

各機關應定期或不定期辦理公務機密檢查，並檢討相關保密機制，透過制度化檢查作業，機先提出預防作為，避免衍生相關洩密事件。

參考法令：

中華民國刑法第 132 條第 1 項

※參照臺灣屏東地方法院 114 年度原簡字第 3 號刑事簡易判決

態樣 2：主管人員洩漏工程預算書檔案

案情概述：

甲為某國際機場股份有限公司副處長，對於該公司依政府採購法規定辦理之工程採購，有執行及監督之權力，屬於依法令從事於公共事務，而具有法定職務權限之公務員。詎甲明知依政府採購法第 34 條規定，機關辦理採購，其招標文件於公告前應予保密，竟利用其職務上之權力，洽採購人員取得含有單價之預算書檔案後，交付給廠商乙，該採購案後續由該廠商之公司得標。

風險評估：

一、 濫用採購主管權力：

機關辦理採購，應以維護公共利益及公平合理為原則，對廠商不得為無正當理由之差別待遇。而採購主管人員亦屬政府採購法規範之採購人員，自然亦應受政府採購法拘束，遵守相關保密規定，不得濫用主管權力，取得並洩漏應保密之採購資訊。

二、 明知故犯應負其責：

採購承辦人員已明確告知該預算書資訊不得提供廠商，甲卻仍將應保密資訊交付廠商，未遵守政府採購法相關保密規範，自應承擔相關刑事責任。

防治措施：

一、 保密義務之認知與加強宣導：

公務員服務法規定，公務員有絕對保守政府機關（構）機密之義務，對於機密事件，無論是否主管事

務，均不得洩漏；離職後，亦同。政府法令繁雜，公務同仁應熟習承辦業務法令，瞭解相關保密規定，同時亦應注意各類政府資訊之使用，避免過失洩漏應保密資訊，另機關亦應加強相關之宣導，強化同仁之保密認知。

二、 加強採購應保密文書管理：

政府採購法訂有相關之保密規範，包含對於招標文件、底價、領標、投標廠商名稱及家數、廠商投標文件、評選委員名單等，均屬刑法所指「中華民國國防以外應秘密」之資訊，各機關應加強對採購應保密文書之管理，避免衍生相關洩密責任。

三、 落實採購人員考核與責任追究：

機關應落實採購人員考核與責任追究，發現有違反採購人員倫理準則之情事者，應依公務員服務法等相關規定處置。其觸犯刑事法令者，應移送司法機關處理，或調離與採購有關之職務、施予與採購有關之訓練。

參考法令：

中華民國刑法第 132 條第 1 項、公務員服務法第 5 條

※參照臺灣桃園地方法院 115 年度簡字第 110 號刑事簡易判決

態樣 3：收受賄賂洩漏 110 報案資訊

案情概述：

甲為警察局勤務指揮中心警員，負責受理民眾 110 報案業務，為具有法定職務權限之公務員，甲明知依規定對 110 報案資料有保密之義務，卻違背其職務，以通訊軟體傳送透過 110 報案系統所獲知死亡案件之亡者死亡方式、地點等應保密資訊，洩漏予殯葬業者乙知悉，使乙得先於其他殯葬業者到場，優先獲取接洽處理殯葬生意之利益，乙並每月定期交付 6 萬元之現金賄款予甲。

風險評估：

一、 通訊軟體洩密不易發覺：

公務人員透過 Messenger、Line 等通訊軟體傳送應保密資訊予業者，僅屬兩人間之私人通訊，基於個人隱私權之保障，若非透過司法偵查手段，外界難以發覺。

二、 違反職務保密義務：

110 報案民眾透過報案系統告知之資訊，藉以回報各勤務單位，由警察、消防隊等立即前往現場處理，以達維護公共利益、社會秩序等法定任務之目的，性質上與國家事務及公共利益攸關，洩漏 110 報案資訊顯已違反職務上應保密之義務。

三、 謀取私利心存僥倖：

私下與殯葬業者聯繫，洩漏職務上應保密資訊，並心存僥倖，以為不會被發現，進而藉以謀取私人不法利益，自應負擔相關法律責任。

防治措施：

一、 定期辦理講座(有獎徵答)及廉政研討會：

聘請非內部單位之專家學者蒞臨演講，並於會後有獎徵答，提升學員的參與感與專注度；另擴大辦理學術研討會，藉由數位專家學者同場探討廉政相關議題，加強同仁之防貪意識並提高警覺。

二、 個人資料安全維護：

公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，主管機關並應定期或不定期稽核公務機關之個人資料保護管理事項實施情形，若發現有缺失或待改善者，應要求提出改善報告。

三、 提供檢舉及揭弊管道：

提供檢舉不法及內部揭弊管道，清楚標示廉政專線、電子信箱及實體收件地址，並強調「身分絕對保密」，以利外部民眾或內部同仁，針對此類洩密或其他不法行為提出檢舉。

參考法令：

一、貪污治罪條例第 4 條第 1 項第 5 款、11 條第 1 項

二、中華民國刑法第 132 條第 1 項

※參照臺灣新北地方法院 114 年度訴字第 832 號刑事判決

態樣 4：非法查詢戶役政系統

案情概述：

甲為某區公所民政課課員，係依法令有法定職務權限之公務員，竟基於非法蒐集個人資料之犯意，假借職務上之機會，利用公務電腦，以其職務上所使用之帳號、密碼，登入戶役政查詢系統，輸入新進同仁乙之身分證字號，以此方式非法蒐集取得乙及其家人之戶役政登記資料。

風險評估：

一、 濫用公務系統查詢權限：

公務機關依業務需求，公務電腦得介接相關公務系統查詢，以利公務同仁業務推行，得申請帳號、密碼登入系統使用，但僅限於公務目的使用，不得基於私人目的，濫用公務查詢系統。

二、 一時好奇應負責任：

好奇心人皆有之，但不能因為一時好奇新進同仁的身分背景，即濫用權限查詢同仁戶役政資料，好奇不能成為免責事由，濫查個資自應負其相應責任。

防治措施：

一、 妥善保管個人公務帳號、密碼：

各種介接之公務查詢系統，應設定查詢人員之帳號、密碼，限制得查詢人員之範圍，不得有多人使用同一帳密情事，公務同仁並應妥善保管個人帳密，不得借給他人使用，每筆查詢紀錄都需對應查詢人員帳號，留存系統查詢數位軌跡。

二、 落實稽核機制：

各機關應建立查詢系統稽核機制，除由主管人員例行抽查外，並應由內部單位定期辦理稽核作業，包括清查有無離職同仁帳號未刪除及異常查詢記錄等，避免不當查詢事件發生。

三、 廉政專案宣導與案例教育：

定期舉辦公務機密與個資法維護講習，以近年違反個資法之真實案例進行宣導，對於個人資料之使用，應提醒同仁予以適當維護管理，若違反個人資料保護法規定，並可能涉及刑事不法或民事賠償責任。

參考法令：

個人資料保護法第 19 條第 1 項、41、44 條

※參照臺灣桃園地方法院 114 年度審簡字第 2142 號刑事簡易判決

態樣 5：傳送陳情資訊於公務群組

案情概述：

甲為某養護工程處約聘人員，為依法令服務具有法定職務權 限之公務員，甲明知依規定對於 1999 陳情系統之陳情人資 料應予保密，甲竟因急於交辦委外廠商，將陳情人姓名、手 機號碼、戶籍地址及陳情事項，以截圖方式傳送至手機通訊 軟體「道路修補平台」公務用群組，而該群組共有 55 人， 其中僅有 3 人為處理該陳情案件之必要人員。

風險評估：

一、 欠缺陳情案件保密認知：

對於 1999 陳情系統之陳情資訊，任意拍照截圖轉傳，未進行任何去識別化或重新編輯處理，顯然欠缺公務保密認知。

二、 使用通訊軟體處理公務：

使用通訊軟體處理事務，具有快速、便捷之效能，但也容易發生洩漏應保密資訊之風險，實務上不乏有相關案例，對於應保密之公共事務，應避免使用通訊軟體處理。

三、 截圖與二次轉傳風險：

工作群組常包含外包廠商、跨單位人員或臨時計畫人員，資料發出後，即可能被非權責人員瀏覽，群組成員可輕易截圖或轉傳至其他群組，縱使發送者後續使用「收回」功能，也無法阻止已被儲存或截圖的資料流出，易衍生資料洩漏風險。

防治措施：

一、 審慎處理陳情案件：

行政院及所屬各機關處理人民陳情案件要點第 18 點規定：「人民陳情案件有保密之必要者，受理機關應予保密。」，陳情書信(包含陳情人身分、陳情內容)對被陳情對象自屬應秘密之文書，不得任意外洩，故任何足以推知陳情人身分、陳情內容之文字、語言、符號皆應予保密，以免危及陳情人之安全，並衍生不必要困擾。

二、 列密處理與去識別化：

陳情案件需會辦他單位、函轉其他機關處理時，若陳情案件有保密之必要者，應以密件處理，必要時並應予遮 蔽或去識別化處理。

三、 避免使用通訊軟體處理公務：

文書處理手冊規定「以電子通信工具傳遞機密文書者，應以加裝政府權責主管機關核發或認可之通信、資訊保密裝備或加密技術傳遞。」，近來實務上屢屢發生因使 用通訊軟體處理公務，導致過失洩漏應保密資訊之案例，使用通訊軟體不可不慎。

四、 加強機關公務機密宣導：

定期舉辦公務機密講習，以近年違反刑法洩漏國防以外秘密消息罪等實際案例進行宣導，加強機關同仁對於公務應保密資訊範圍及刑事責任之認知。

五、 製作宣導摺頁及標語：

將生硬的法律條文轉化為易讀、有感且具警示效果的文宣，以達到深化廉政意識的目的，情境誤區（吸睛引導)，用簡短的漫畫或對話框，點出日常公務或與民眾互動中「最容易誤觸的灰色地帶」(例如：年節送

禮、飲宴應酬、小額核銷），粘貼於同仁之出入口明顯位置，以時時提醒防貪之重要性。

一、 **參考法令**：刑法第 132 條

※參照臺灣高雄地方法院 112 年度簡字第 2370 號刑事判決

態樣 6：無故竊錄他人非公開活動

案情概述：

甲前為某大學助理教授，明知審議研究升等著作係秘密會議，會議過程均為保密，僅有審查委員能進入會議室進行討論審查，竟為知悉審查教師升等案件之不公開會議討論內容，基於妨害秘密之犯意，先將具即時觀看功能之智能攝影機藏放在該學程之會議室內之水槽櫃下方隱蔽處，並連接該會議室電源，而以此方式無故竊錄升等審查會議之非公開活動、言論、談話內容，而得知該次升等審查會議審議內容。

風險評估：

一、 明知故犯應負其責：

行為人身為助理教授，明知審議研究升等著作係秘密會議，會議過程均為保密，本應恪遵法規，卻為個人私利，為得知該次升等審查會議審議本人之研究升等而遂行不法，自應承擔相關刑、民事責任。

二、 會議室空間管控不足：

學校內部人員進出會議室未予管控，學校空間若未妥善管理，易衍生資料失竊、遺失或洩漏風險。

防治措施：

一、 建立機關安全維護機制：

機關應建立內部安全維護機制，例如設置保全人員、進出人員登記管制、攝影監控系統、廁所及更衣室緊急求救系統建置、與當地警察機關加強聯繫等。

二、 落實會議室等空間管理：

會議室借用應落實登記程序，並有專責人員管理，未使用時應確實上鎖，避免人員任意進出，衍生管理風險，並維護機關同仁安全。

三、 辦理機關安全檢查：

實體重點區域（會議室、廁所）檢查、採定期及不定期方式，檢查是否有不合理的微孔、異常多餘的線材、不常在該處出現的日常物品（如包裝異常的偽裝隨身碟、鬧鐘、電源轉接頭），降低遭側錄的風險，維護機關同仁安全。

四、 辦理實務案例宣導：

每年定期舉辦個資法宣導，直接引用「偷拍」、「涉及散布、播送或販賣竊錄內容」等真實判決，打破「以為沒人知道」的僥倖心理。

五、 強化機關安全管制：

「做好門禁管制，加強辨證」以防範不法冒名、洩密及竊資等貪瀆或危害事件發生，在進入機關辦公區，務必登記換證需有相關部門員工引導，切勿讓外人於內部流竄，造成機敏資料外洩。

參考法令：

中華民國刑法第 315 條之 1 第 2 款

※參照臺灣臺北地方法院 114 年度審簡字第 1551 號刑事判決

態樣 7：利用非法查詢個人資料提告

案情概述：

甲為某警察局民防管制中心技佐，具有公務員之身分，其依職權得輸入個人公務帳號後，登入內政部警政署知識聯網，查詢相關資料，緣甲因故與乙產生糾紛，嗣後甲為對乙提出刑事告訴，竟使用公務電腦登錄警政知識聯網，將含有乙個資之國民身分證統一編號、行動電話號碼等相關資料下載並列印成紙本，並持上開紙本至派出所對乙提告。

風險評估：

一、濫用公務系統查詢權限：

公務機關介接之公務查詢系統，可查詢資料包括姓名、國民身分證統一編號、行動電話號碼等資料，屬於個人資料保護法第 2 條第 1 款所規範之個人資料，不得任意非法蒐集、利用，公務同仁應於執行法定職務範圍內使用系統，並與蒐集之目的相符，不得基於私人目的，濫用公務查詢系統。

二、未循正當管道取得個資：

甲為提告需使用之個人資料，本可透過聲請受理機關調查證據等合法程序取得，而非私自利用公務帳號查詢，甲捨合法之調查途徑，逕自利用職權蒐集、利用個人資料，手段已逾越達成目的之必要程度。

防治措施：

一、妥善保管個人公務帳號、密碼：

各種介接之公務查詢系統，應設定查詢人員之帳號、密碼，限制得查詢人員之範圍，不得有多人使用同一帳密情事，公務同仁並應妥善保管個人帳密，不得借給他人使用，每筆查詢紀錄都需對應查詢人員帳號，留存系統查詢數位軌跡。

二、 建置自動警示功能：

非上班時間查詢、密集查詢同一人、查詢名人/政治人物查詢非自己承辦區域資料，只要觸動上述指標，系統就會自動發出資安警示，並將警示情形即時連線至資安與政風單位，提高防範。

三、 定期辦理專案稽核：

由機關內的政風室與資訊單位成立聯合稽核小組，定期進行專案稽核，針對「查詢非本轄區民眾」、「連續高頻查詢」、「夜間或非上班時間存取」等異常查詢紀錄進行稽核作業。

四、 加強法令宣導：

利用機關內公開會議或舉辦法令講習，適時宣導相關案例，深化同仁對於個人資料保護法及保密知識。

參考法令：

個人資料保護法第 15、41、44 條

※參照臺灣彰化地方法院 115 年度簡字第 2 號刑事簡易判決