個資外洩案件行政調查作業手冊

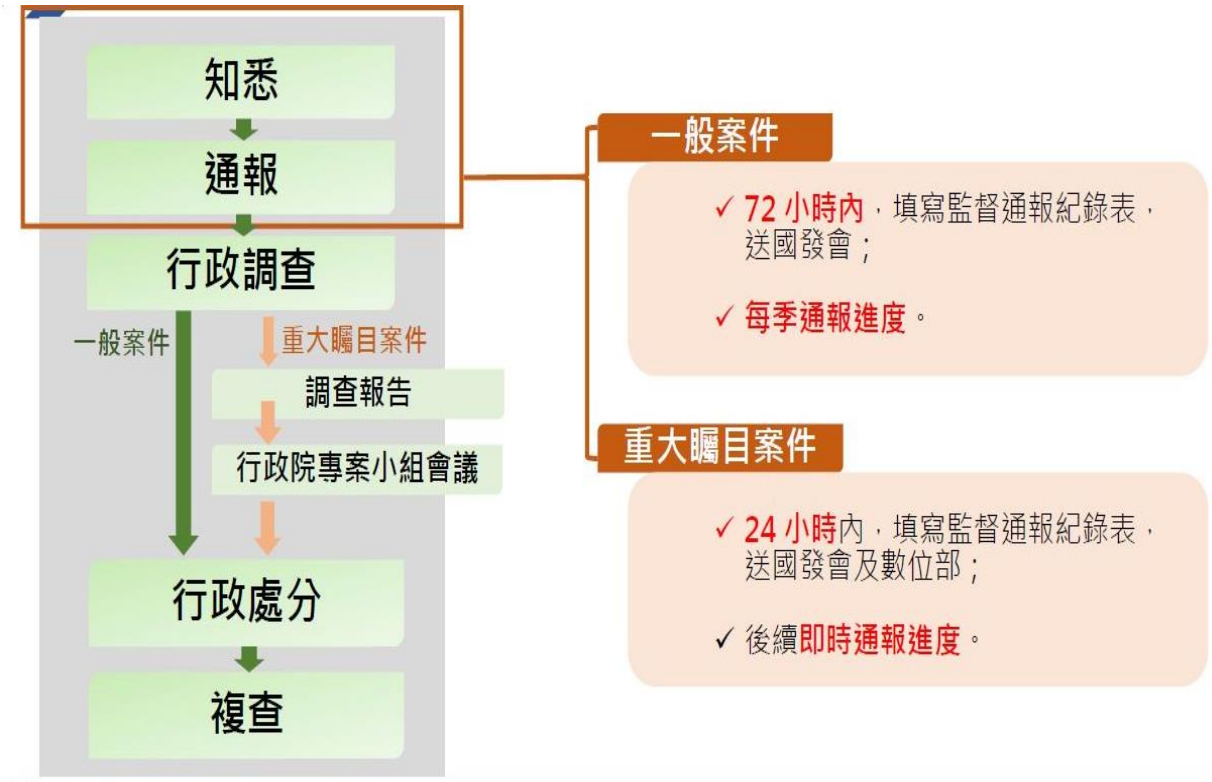
目錄

壹、 受理個資外洩案件，進行監督通報程序 3
一、 一般個資外洩案件監督通報程序 3
(一) 首次知悉外洩事故之時間、方式及內容之監督通報 3
(二) 後續提送監督通報之時點 4
二、 重大矚目個資外洩案件監督通報程序 4
(一) 重大矚目案件之定義 4
(二) 首次知悉外洩事故之時間、方式及內容之監督通報 4
(三) 後續提送監督通報之時點 5

貳、 啟動個資外洩案件之後續監督管理措施 5
一、 通用事項 6
(一) 行政措施及處置 6
1. 行政調查基本原則 6
(1) 適當性 6
(2) 必要性 6
(3) 狹義比例原則 6
2. 個資人資料保護法(以下簡稱個資法)規定之行政措施及處置類型 6
(1) 第一類型之行政措施及處置 7
(2) 第二類型之行政措施及處置 7
(3) 遵循行政措施及處置之義務及違反之行政罰 10
(4) 行政措施及處置之實務討論 11
3. 請求警察機關或法務部調查局提供協助 13
4. 完整紀錄行政調查過程，以利後續事實釐清與評估做成相關行政處分 14
(二) 調查事實整理 15
1. 外洩事故機關與關連機關 15
2. 外洩事故描述 15
3. 外洩事故類型分析 15
4. 受影響個人資料類別及損害評估 15

5. 非公務機關通知當事人之情形 15
6. 非公務機關採取應變措施 15
(三) 分析原因與處置措施 16
1. 事故發生原因分析 16
2. 個資安全維護義務法律遵循分析 16
3. 採取之個資法賦予權限，積極進行相關裁罰或相關行政處分 16
4. 待改善事項方案及建議作為 16
5. 命令改正時程及查核追蹤機制 16
二、 重大矚目案件特殊事項 17
(一) 調查期程 17
(二) 偕同數位發展部辦理行政調查 18
(三) 行政調查報告撰寫及後續事項 18
1. 10 日內完成調查報告 18
2. 調查報告應送國發會及數位發展部，必要時國發會得報請行政院指定之政務委員，原則於 2 週內召開會議，聽取行政調查辦理情形 18
3. 調查報告是否公開 18
附件 1 個人資料安全稽核檢查表 19
附件 2 個資外洩重大矚目案件調查報告格式 29

壹、 受理個資外洩案件，進行監督通報程序



一、 一般個資外洩案件監督通報程序

(一) 首次知悉外洩事故之時間、方式及內容之監督通報

行政院及所屬各機關落實個人資料保護聯繫作業要點(以下簡稱聯繫作業要點)第 7 點第 1 項

中央目的事業主管機關接獲非公務機關通報或副知，或非因通報或副知而自行知悉個資外洩案件，經確認屬該機關管轄後，應於接獲通報、副知或知悉時起 72 小時內，填列監督通報紀錄表，通報國發會。但個資外洩案件屬重大矚目者，依第 8 點規定辦理。

(二) 後續提送監督通報之時點

聯繫作業要點第 7 點第 2 項

中央目的事業主管機關應就前項本文之個資外洩案件之後續行政措施及處置情形，按季通報國發會。

二、 重大矚目個資外洩案件監督通報程序

(一) 重大矚目案件之定義

聯繫作業要點第 2 點第 2 項

本要點所定重大矚目之個資外洩案件，其範圍如下：

(一)行政院、立法院或監察院關注之個資外洩案件。

(二)經媒體顯著披露之個資外洩案件,例如經平面媒體全國性版面報導、電子媒體專題討論。

(二) 首次知悉外洩事故之時間、方式及內容之監督通報

聯繫作業要點第 8 點第 1 項

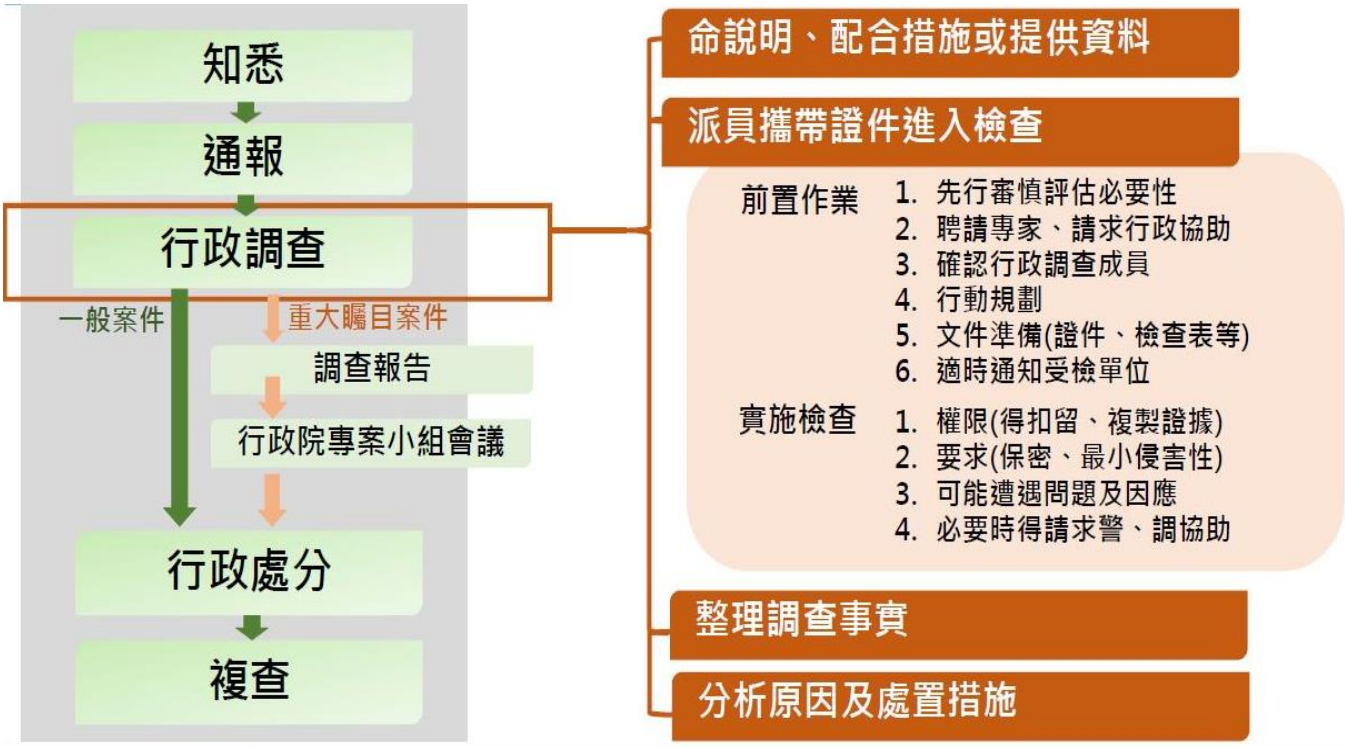
前點第 1 項但書之個資外洩案件屬重大矚目者，中央目的事業主管機關經確認屬該機關管轄後，應於接獲通報、副知或知悉時起 24 小時內，填列前點第 1 項本文所定監督通報紀錄表，通報國發會及數位發展部。

為加速重大矚目之個資外洩案件之首次通報時程，及強化數位發展部之協助角色，使該部亦接受重大矚目之個資外洩案件與後續行政措施及處置情形之通報。

（三）後續提送監督通報之時點

聯繫作業要點第 8 點第 4 項 中央目的事業主管機關應就重大矚目之個資外洩案件後續行政措施及處置情形，即時通報國發會及數位發展部。

貳、 啟動個資外洩案件之後續監督管理措施



一、 通用事項

(一) 行政措施及處置

1. 行政調查基本原則

依據行政程序法第 34 條、第 36 條、第 37 條規定，行政調查開始和執行方式原則為職權調查，調查之開啟與進行乃行政機關職權進行的範疇；而對於是否發動行政檢查，即必要性判斷，一般以比例原則進行評估，關於比例原則三個子原則如下：

(1) 適當性：國家採取的行為須有助於目的的達成。

(2) 必要性：若有多種措施均可達成目的，應選擇侵害最小者，又稱「最小侵害原則。

(3) 狹義比例原則：國家採取的手段對人民的侵害和所欲達成的目的，兩者間不能顯失公平，又稱「衡平性原則」。

2. 個資人資料保護法(以下簡稱個資法)規定之行政措施及處置類型

聯繫作業要點第 9 點第 1 項提醒個資法賦予中央目的事業主管機關得對該非公務機關為適當監督管理措施之重要權限，以下擇個資法第 22 條至第 24 條規定及簡要說明，最後再輔以行政措施及處置之實務討論。

兩大類型之行政措施及處置

個資法第 22 條第 1 項

中央目的事業主管機關或直轄市、縣（市）政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。

為落實個人資料之保護，應賦予監督機關有命令、檢查及處分權，個資法規定中央目的事業主管機關或直轄市、縣（市）政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入該非公務機關檢查或要求說明、提供相關證明資料，以強化監督機關之權責。故依行政措施及處置類型之層次，可分為兩大類：第一、「得命相關人員為必要之說明、配合措施或提供相關證明資料」(以下簡稱「第一類型之行政措施及處置」)；第二、「得派員攜帶執行職務證明文件，進入檢查」(以下簡稱「第二類型之行政措施及處置」)。

(1) 第一類型之行政措施及處置：包含「得命說明」、「得命配合措施」、「得命提供相關證明資料」等相關處分，規定於個資法第 22 條第 1 項後段。

(2) 第二類型之行政措施及處置：

> ① 扣留或複製
>
> 個資法第 22 條第 2 項
>
> 中央目的事業主管機關或直轄市、縣（市）政府為前項檢查時，對於得沒入或可為證據之個人資料或其檔案，得扣留或複製之。對於應扣留或複製之物，得要求其所有人、持有人或保管人提出或交付；無正當理由拒絕提出、交付或抗拒扣留或複製者，得採取對該非公務機關權益損害最少之方法強制為之。

檢查人員發現非公務機關違反本法規定，如將所有儲存媒介物設備予以查扣，恐有違比例原則，爰規定檢查時依行政罰法相關規定發現得沒入或可為證據之個人資料或檔案，而有扣留或複製之必要者，得予扣留或複製之。此外，以電腦儲存之資料檔案，其消磁、刪除或移轉非常快速，如檢查時未能即時扣留或複製，該違法資料或證據極易被湮滅或消除，檢查機關亦得依行政罰法相關規定，要求應扣留或複製物之所有人、持有人或

保管人提出或交付，且於遇有無正當理由拒絕提出、交付或抗拒扣留或複製者，得強制為之，但應採取對該非公務機關權益損害最少之方法，以避免違反比例原則，例如：得複製檔案時，即無需予以扣留。

另個資法施行細則第 30 條規定：「依本法第 22 條第 2 項規定，扣留或複製得沒入或可為證據之個人資料或其檔案時，應掣給收據，載明其名稱、數量、所有人、地點及時間。(第 1 項)依本法第 22 條第 1 項及第 2 項規定實施檢查後，應作成紀錄。(第 2 項)前項紀錄當場作成者，應使被檢查者閱覽及簽名，並即將副本交付被檢查者；其拒絕簽名者，應記明其事由。(第 3 項)紀錄於事後作成者，應送達被檢查者，並告知得於一定期限內陳述意見。(第 4 項)」

② 協助之人員

個資法第 22 條第 3 項

中央目的事業主管機關或直轄市、縣（市）政府為第 1 項檢查時，得率同資訊、電信或法律等專業人員共同為之。

被檢查之個人資料檔案，有可能以不同方式儲存於各種類型媒介物，如未具有相當專業知識，勢必無法達成檢查目的，爰規定檢查機關得率同資訊、電信或法律等專業人員共同進行檢查。

③ 保密義務

個資法第 22 條第 5 項

參與檢查之人員，因檢查而知悉他人資料者，負保密義務。

為確保個人資料之隱私性，避免資料當事人二度受到傷害，明定因檢查而知悉他人資料者，應負保密義務，不得洩漏。另個資法施行細則第 29 條

規定：「依本法第 22 條規定實施檢查時，應注意保守秘密及被檢查者之名譽。」

④ 扣留物或複製物之處理

個資法第 23 條

對於前條第 2 項扣留物或複製物，應加封緘或其他標識，並為適當之處置；其不便搬運或保管者，得命人看守或交由所有人或其他適當之人保管。

扣留物或複製物已無留存之必要，或決定不予處罰或未為沒入之裁處者，應發還之。但應沒入或為調查他案應留存者，不在此限。

明定扣留物或複製物應加具識別之標示，並為適當之處理，以確保其安全。另扣留物或複製物除應沒入或因調查他案而有留存之必要者，應繼續扣留外，如無必要留存，或決定不予處罰或未為沒入之裁處者，應即發還，以保障民眾權益。

⑤ 特殊救濟程序

個資法第 24 條

非公務機關、物之所有人、持有人、保管人或利害關係人對前 2 條之要求、強制、扣留或複製行為不服者，得向中央目的事業主管機關或直轄市、縣（市）政府聲明異議。

前項聲明異議，中央目的事業主管機關或直轄市、縣（市）政府認為有理由者，應立即停止或變更其行為；認為無理由者，得繼續執行。經該聲明異議之人請求時，應將聲明異議之理由製作紀錄交付之。

對於中央目的事業主管機關或直轄市、縣（市）政府前項決定不服者，僅得於對該案件之實體決定聲明不服時一併聲明之。但第 1 項之人依法不得對該案件之實體決定聲明不服時，得單獨對第 1 項之行為逕行提起行政訴訟。

當事人或物之所有人、持有人、保管人、利害關係人，對檢查或扣留、複製資料檔案行為認有違法或不當時，應有表示不服聲明異議之權利，以為救濟。對於當事人等聲明之異議，執行檢查之機關認有理由者，應立即停止或變更其行為；認無理由者，得繼續執行。但因當事人等得於日後對此檢查或其他強制、扣留或複製行為，提起救濟，是以經其請求時，應將聲明異議之理由製作紀錄交付之，不得拒絕。當事人等對於聲明異議之決定不服時，僅得於對該案件之實體決定聲明不服時一併聲明之，不得單獨提起救濟；至於當事人等依法不得對該案件之實體決定聲明不服時，則可單獨對第 1 項之檢查、扣留、複製或其他強制行為，逕行提起行政訴訟，以保障其權利。

(3) 遵循行政措施及處置之義務及違反之行政罰

① 非公務機關及其相關人員應遵循行政措施及處置義務

個資法第 22 條第 4 項

對於第 1 項及第 2 項之進入、檢查或處分，非公務機關及其相關人員不得規避、妨礙或拒絕。

② 非公務機關及其相關人員違反應遵循行政措施及處置義務之行政罰

個資法第 49 條

非公務機關無正當理由違反第 22 條第 4 項規定者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣 2 萬元以上 20 萬元以下罰鍰。

為強化目的事業主管機關執行本法職務之職權，個資法課予非公務機關及其相關人員應遵循主管機關依個資法第 22 條第 1 項及第 2 項進入、檢查或處分之義務。

違反個資法第 22 條第 4 項規定之義務者，除依個案判斷有正當阻卻違法之理由外，目的事業主管機關即應按次處罰。

(4) 行政措施及處置之實務討論

① 第一類型之行政措施及處置

通知受調查對象為必要之說明、配合措施及提供相關證明資料說明時，倘遭遇下列問題，建議方式：

A. 如何確保受調查對象有收受通知？

機關可評估以掛號的方式寄送重要的公文通知，以確保通知有效送達相對人。

B. 受調查對象消極不回覆應如何處理？

依據個資法第 22 條正式命其為必要之說明、配合措施或提供資料之處分，並敘明倘仍未依限回復，則依個資法第 49 條為相關裁罰。

② 第二類型之行政措施及處置

A. 派員進入調查前置準備

a. 審慎評估後陳報

b. 視具體個案聘請專家、以書面方式請求其他機關的行政協助：

因非公務機關類型多元，所涉業務多元，倘經評估須經專家或其他機關協助，機關部分應依據行政程序法第 19 條為之。

c. 確認行政調查組成人員：

依據聯繫作業要點第 4 點規定，中央目的事業主管機關應組成個資行政檢查小組，辦理年度行政檢查，及因應、處理個資外洩案件；其成員得包括具有法律、資訊專業之機關資深人員及外部專家。爰原則上，行政調查人員即為各主管機關之個資行政檢查小組成員，惟得依個案情形調整納入相關業務人員、外部專家或非公務機關所在地之直轄市、縣(市)政府派員參與。

d. 行政調查前期行動規劃：

進行調查前，為降低調查過程可能遭逢的阻礙以及調查的效率，建議調查前可先行沙盤推演，並為行動規劃。

e. 文件準備：

a) 執行職務證明文件(含身分證明文件)。

b) 個人資料安全稽核檢查表(詳附件 1)

c) 複製物或扣留物之收據。

d) 其他必要文件。

f. 依案件性質，適時通知受檢單位：

為避免突襲，並踐行行政程序相對人之程序保障，主管機關可視具體個案情形，以書面通知被調查人行政調查時間、調查場所、調查目的、得否委託他人到場，以及不到場之法律效果。如情況緊急，如不立即調查，將可能發生無法回復的重大損害時，可選擇以電話方式為通知，惟宜作成電話紀錄單，後續如生爭議時（如被調查人爭執調查程序有瑕疵等情），可作為證據之用。

B. 實施進入調查

a. 權限

a) 發動個資行政調查。

b) 率同資訊、電信或法律等專業人員陪同為之。

c) 要求被調查人配合調查。

d) 對於得沒入或可為證據之個人資料或其檔案，得扣留或複製。

b. 要求

a) 保密要求。

b) 檢查手段應具最小侵害性。

c) 對於扣留物或複製物為適當的處置或保管；如無扣留的必要，應發還。

C. 可能遭遇問題

實施行政調查過程中，因具體個案的不同，可能會面臨問題也會

有所差異，實施進入查察時，例示可能遭遇問題以及評估解決的方式

a. 被調查人拒絕進入查察：

被調查人可能會以「檢查過於臨時，資料尚未備齊，需準備時間」或「檢查將嚴重影響業務運作」等事由拒絕進入檢查。可能因應作法如下：

個資法第 22 條並無授予目的事業主管機關強行進入之權力，除紀錄上開拒絕進入相關情形，以供將來是否作成個資法第 49 條規定裁罰的判斷依據外，如現場仍有非公務機關相關人員，並將其拒絕進入理由記明筆錄，由被調查人簽名確認。

b. 被調查人同意進入調查，但拒絕說明以及拒絕配合調查：

倘被調查人雖同意進入檢查，但檢查人面臨實際個案的具體情狀時，仍須被調查人配合進行說明或協助檢查。若被調查人以「消極」的方式配合，會導致檢查過程多有阻礙的情況。此時，主管機關當可評估基於個資法的授權，可考慮在對被調查人權益最小的情況下行使強制手段，例如扣留或複製得沒入或可為證據之個人資料或其檔案，但仍應注意個案進行中比例原則的操作。

被調查人及相關人員無正當理由拒絕說明與配合檢查，也不提出相關資料時，檢查人得將要求提出而被調查人拒不提出之資料與具體情況記明，並於檢查結束後，要求被調查人簽名並給予陳述意見之機會，作為將來是否作成個資法第 49 條的判斷依據。

3. 請求警察機關或法務部調查局提供協助

聯繫作業要點第 9 點第 2 項

中央目的事業主管機關就個資外洩案件辦理行政調查，得於必要時請求警察機關或法務部調查局提供協助。

中央目的事業主管機關就個資外洩案件辦理行政調查，得於必要時(例如涉及刑事犯罪)，請求警察機關或法務部調查局提供協助。換言之，中央目的事業主管機關若因執行職務知有犯罪嫌疑者，應為告發(刑事訴訟法第 241 條規定)；若係需行政協助，則依行政程序法第 19 條規定為之。

另補充說明兩點如下：

第一、辦理個資外洩案件行政調查，非公務機關違反個資安全維護義務之行為，係行政罰而非刑事罰，上開所稱涉及刑事犯罪，係指他人而非該「非公務機關」，非同一行為人，並無行政罰法第 26 條「刑事處罰優先行政處罰」規定之適用。故即使司法警察仍在進行刑事調查，個資法之行政調查仍不得停止。

第二、若係請求警察協助維持目的事業主管機關進入非公務機關場域執行行政調查之安全秩序，則內政部警政署(下稱警政署)支援事項及程序如下表格，惟請注意警力僅用於維持秩序及保護調查人員安全，不參與調查過程：

目的事業主管機關	請求警察協助事項
未至非公務機關場域前	● 於有具體情資研判現場有妨礙調查或公共秩序之虞時，得請警察單位協助。 ● 於符合前開情況下，非例假日進行行政調查者，依行政程序法第 19 條函請地方警察機關(地方政府警察局)行政協助；例假日或急迫情況未及以書面函請其協助時，可洽警政署協助聯繫。
已至非公務機關場域時	現場如遇突發情況，撥打 110 請求警力支援。

4. 完整紀錄行政調查過程，以利後續事實釐清與評估做成相關行政處分

(1) 紀錄行政調查前準備：

例如：行政調查小組分工(含參與調查機關或協助者之角色)、規劃行政調查期程、與受調查非公務機關連繫情形及是否請受調查機關提供相關資料或自評等。

(2) 紀錄行政調查情形：

包含行政調查之時間、調查方式、調查範圍、調查項目、調查發現(含技術面、管理面等)、是否對廠商提出改正要求(是否進行改正處分)、受調查事業改正情形、後續複查等時程規劃、複查結果、是否將進行下階段處分、是否將再次命改正等相關事宜。

(二) 調查事實整理

1. 外洩事故機關與關連機關：

說明經調查後，本起外洩事故主體為何，若有其他關連機關(如：有受託機關、委託機關等)，請列出並說明其他關連機關於外洩事故涉及個資之角色。

2. 外洩事故描述：

整理說明本次外洩事故情形，含經過、時間、事故主體與關連機關之作為等。

3. 外洩事故類型分析：

屬被竊取、竄改、毀損、滅失、洩漏或為其他侵害事故。

4. 受影響個人資料類別及損害評估：

一般或特種個人資料、個資內容類別描述、個資侵害筆數、詐騙金額或其他侵害情形評估。

5. 非公務機關通知當事人之情形：

非公務機關遵循個資法規定通知當事人之時間、方式及通知內容，若有佐證資料請一併紀錄。

6. 非公務機關採取應變措施：

非公務機關已採取或即將採取之應變措施，應包含技術面、管理面等，若有佐證資料請一併紀錄。

（三）分析原因與處置措施

1. 事故發生原因分析：

調查後就事故發生原因之分析及判斷，例如評估該事故如何對個人資料造成侵害、造成何種侵害及程度、直接原因及間接原因等。

2. 個資安全維護義務法律遵循分析：

判斷事故主體及/或關聯機關是否已盡個資法第 27 條安全維護義務個資法施行細則第 12 條規定或符合其所應適用之個資檔案安全維護辦法規定等。另針對非公務機關有無踐行個資法第 12 條及施行細則第 22 條規定，亦應併同檢視分析。

3. 待改善事項方案及建議作為：

同時擬定對非公務機關應改善事項方案及建議作為，包含技術面、管理面等。

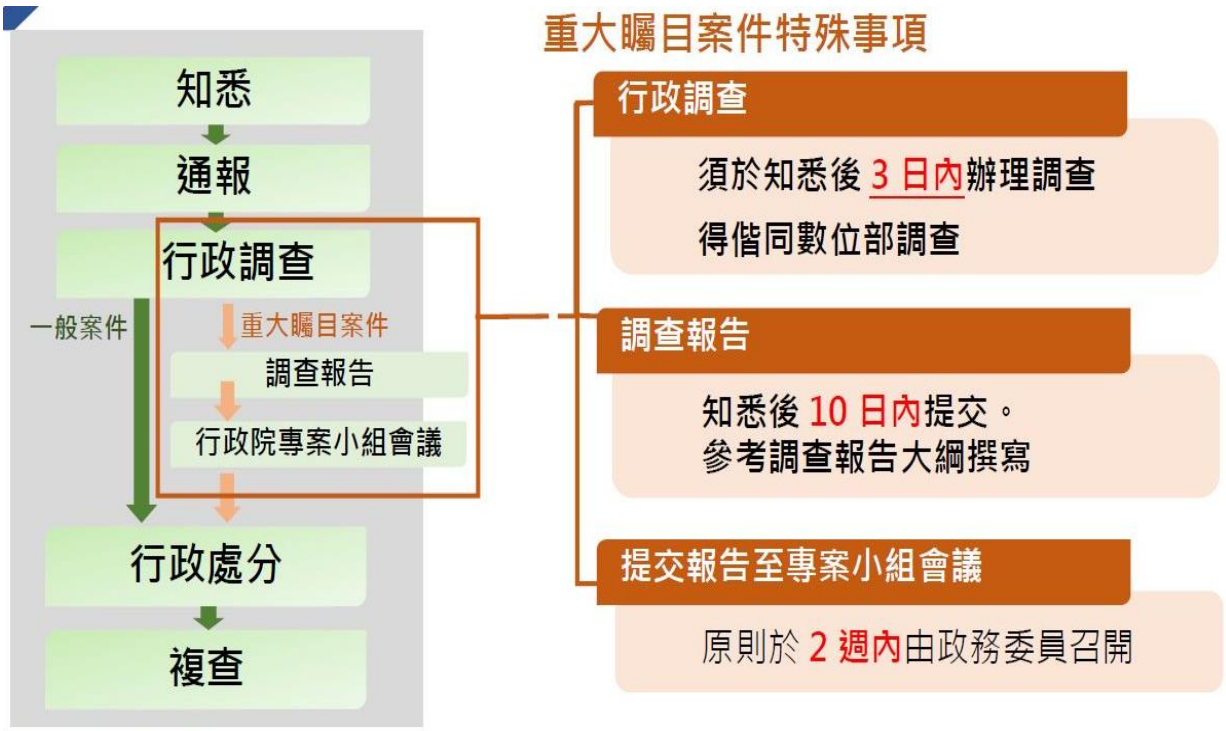
4. 採取之個資法賦予權限，積極進行相關裁罰或相關行政處分：

個資法第 25 條、第 48 條第 2 項及第 3 項、第 49 條及第 50 條規定。

5. 命令改正時程及查核追蹤機制：

以行政處分命非公務機關限期改正，並持續查核追蹤，若仍未改正，按次依個資法第 48 條規定處罰。

二、 重大矚目案件特殊事項



(一) 調查期程

3 日內進行行政調查，10 日內完成調查報告，原則上由行政院指定之政務委員於 2 週內召開會議，聽取行政調查辦理情形

聯繫作業要點第 8 點第 2 項

中央目的事業主管機關針對前項重大矚目之個資外洩案件及依前點第 1 項本文規定通報後改列為重大矚目案件者，應於接獲通報、副知或知悉時起 3 日內進行行政調查，10 日內完成調查報告，報告完成後應送國發會及數位發展部；必要時國發會得報請本院指定之政務委員，原則於 2 週內召開會議，聽取行政調查辦理情形。

增訂有關中央目的事業主管機關針對重大矚目之個資外洩案件之行政調查及其作業時程之規定，及明定本院指定之政務委員必要時得召開會議聽取中央目的事業主管機關之行政調查辦理情形規定。

若中央目的事業主管機關於調查過程，認須請非公務機關先進行自評，則應考量重大矚目案件之急迫性，給予合宜之自評時間，時間不宜過長，以免影響相關調查之續行。

(二) 偕同數位發展部辦理行政調查

> 聯繫作業要點第 8 點第 3 項
>
> 中央目的事業主管機關得偕同數位發展部辦理前項之行政調查。

為協助中央目的事業主管機關提升行政檢查量能，中央目的事業主管機關辦理重大矚目個資外洩案件之行政調查，得偕同數位發展部為之。

(三) 行政調查報告撰寫及後續事項

1. 10 日內完成調查報告

調查報告格式詳附件 2，內容包含：基本資訊、24 小時內監督通報過程、3 日內開始行政調查迄今之行政作為、調查事實整理、分析原因與處置措施、個案調查綜合分析、建議與結論等。

2. 調查報告應送國發會及數位發展部，必要時國發會得報請行政院指定之政務委員，原則於 2 週內召開會議，聽取行政調查辦理情形

會議由國發會發開會通知，由相關中央目的事業主管機關準備簡報說明。

3. 調查報告是否公開

中央目的事業主管機關所完成之調查報告，亦屬政府資訊，因此，應先行考量是否具有政府資訊公開法第 18 條應限制公開或不予提供之事由，始得公開或對外提供。

附件 1 個人資料安全稽核檢查表

個人資料安全稽核檢查表-_____(填表單位)

填表說明：

一、 稽核結果欄：依稽核實際狀況，參考相關佐證資料填具查核結果。

(一) 符合:實際作業已依稽核內容訂定相關規範,並已有相關實作紀錄,或已建立標準規範而尚未有實際作業。

(二) 不符合：未完全依稽核內容要求訂定相關程序，或未完全依相關程序執行並產生實作紀錄；並請於說明欄儘可能詳述未符合之情形與樣態。

(三) 不適用：實際作業排除稽核內容之適用 。

二、 說明欄位：應記錄稽核之參考佐證資料或簡述實際作業狀況。

稽核項目	稽核內容	查核結果	說明	備註
1.配置管理之人員及相當資源	1.1 是否設個人資料管理單位或適當組織？	□符合 □不符合 □不適用		請檢附個資管理單位組織圖、分工及相關辦法，並提出個資窗口所協助之各項個資保護工作事項,如：參與會議、盤點及風險評鑑工作、事件處理等。
2.界定個人資料之範圍	2.1 是否每年定期清查其所保有之個人資料檔案及其蒐集、處理或利用個人資料之作業流程,據以建立個人資料檔案清冊及個人資料作業流程說明文件？	□符合 □不符合 □不適用		請檢附個人資料檔案清冊及個人資料作業流程說明文件，並經權責主管核定之紀錄。

稽核項目	稽核內容	查核結果	說明	備註
3.個人資料之風險評估及管理機制	3.1 是否每年定期評估其因蒐集、處理或利用個人資料可能面臨的法律或其他風險，並訂定適當之管控及因應措施？	□符合 □不符合 □不適用		請檢附風險評估過程底稿、風險評鑑報告及風險處理計畫。
4.事故之預防、通報及應變機制	4.1 個資事故應變機制是否包含降低、控制事故對當事人造成損害之作法？	□符合 □不符合 □不適用		請說明應變機制對降低、控制事故對當事人造成損害之作法
	4.2 個資事故應變機制，是否包含適時以電子郵件、簡訊、電話或其他便利當事人知悉之適當方式，通知當事人事故之發生與處理情形，及後續供當事人查詢之專線與其他查詢管道？	□符合 □不符合 □不適用		請說明應變機制對通知當事人之作法
	4.3 個資事故應變機制，是否包含避免類似事故再次發生之矯正及預防機制？	□符合 □不符合 □不適用		請說明應變機制對避免類似事故再次發生之矯正及預防機制。
	4.4 是否就個資事件之重大事故定義，及重	□符合 □不符合 □不適用		請檢附事故通報文件

稽核項目	稽核內容	查核結果	說明	備註
	大事故之通報流程為何？			
5.蒐集、處理、利用作業	5.1 資料蒐集、處理是否具備特定目的並具有法定要件？	□符合 □不符合 □不適用		請檢附最新個資盤點資料，確認皆已識別保有依據。
	5.2 個人資料之利用，是否符合特定目的之範圍？	□符合 □不符合 □不適用		請檢附最新個資盤點資料，確認皆已識別保有依據。
	5.3 是否有目的外之利用？目的外利用是否符合法定要件？	□符合 □不符合 □不適用		請說明機關所蒐集之個資是否具有目的外之利用情形。如有目的外利用，請說明其符合之法定要件。
	5.4 是否依規定取得當事人同意（當事人同意之情形）？	□符合 □不符合 □不適用		請說明蒐集個資並取得當事人同意之情形。
	5.5 是否履行告知義務（未履行告知義務時，是否符合免告知之情形）？	□符合 □不符合 □不適用		請檢附告知事項。
	5.6 是否已於首次行銷時提供當事人表示拒絕行銷之管道？如需費用是由機關支付所需費用？	□符合 □不符合 □不適用		請說明提供當事人拒絕行銷之方式。

稽核項目	稽核內容	查核結果	說明	備註
	5.7 是否依當事人拒絕接受行銷之要求，立即停止利用其個人資料為行銷，並周知所屬人員或採行防範所屬人員再次行銷之措施？	□符合 □不符合 □不適用		請說明是否有當事人拒絕接受行銷以及作業流程。
6. 資料安全管理及人員管理	6.1 是否識別業務內容涉及個人資料蒐集、處理或利用之人員？	□符合 □不符合 □不適用		請檢附個資管理單位組織圖、分工及相關辦法，以及個人資料檔案清冊。
	6.2 是否依其業務特性、內容及需求，設定所屬人員接觸消費者個人資料之權限，並定期檢視其適當性及必要性？	□符合 □不符合 □不適用		請檢附個資系統權限申請表單以及帳號權限審查紀錄。
	6.3 是否與所屬人員約定保密義務？	□符合 □不符合 □不適用		請檢附所屬人員清單(正職、短期約僱)及所簽署之保密切結書。
	6.4 是否要求人員離職時，返還保有消費者個人資料之載體，並刪除因執行業務而持有之消費者個人資料？	□符合 □不符合 □不適用		請檢附所屬人員清單(正職、短期約僱)及所簽署之保密切結書或離職單。

稽核項目	稽核內容	查核結果	說明	備註
	6.5 消費者個人資料有加密之必要者，於蒐集、處理或利用時，是否採取適當之加密措施？	□符合 □不符合 □不適用		請說明針對個資電子檔案之控管規範，例如將個人資料檔案置於公用電腦或網路共用資料夾，是否進行加密或遮蔽？並檢附查核結果。
	6.6 傳輸消費者個人資料時，是否依不同傳輸方式，採取適當之安全措施？	□符合 □不符合 □不適用		請說明機關對外傳送個資檔案之相關規範，檢附規範制度文件。例如以電子郵件傳送敏感之個資檔案時，是否採加密機制？並請相關佐證。
	6.7 消費者個人資料有備份之必要者，是否對備份資料採取適當之保護措施？	□符合 □不符合 □不適用		請說明資料備份機制，並檢附規範制度文件。
7.認知宣導及教育訓練	7.1 是否定期對實施所屬人員之個人資料保護與管理認知宣導及教育訓練？所屬人員是否明瞭上課內容？	□符合 □不符合 □不適用		請檢附對所屬人員之教育訓練簡報、各項相關課程簽到表(需含授課日期)及課後評量結果。上課內容應包含個人資料保護相關法令之要求、人員之責任範圍及各項個人資料保護相關作業程序。
8.設備安全管理措施	8.1 是否依據作業內容及環境之不同，實施必要之安全環境管制？	□符合 □不符合 □不適用		請說明對存放儲存媒介物之環境相關消防、監控、進出入等控管措施，並檢附相關照片。
	8.2 是否妥善維護並控管個人資料蒐集、處理或利用過程	□符合 □不符合 □不適用		請確認是否定期檢查或維護更新設備？並請檢附定期檢查及維護紀錄。

稽核項目	稽核內容	查核結果	說明	備註
	中所使用之實體設備？			
	8.3 是否針對不同作業環境，建置必要之保護設備或技術？	□符合 □不符合 □不適用		請檢附消防、監控設備等維護紀錄。
9. 資料安全稽核機制	9.1 是否每年定期由適當組織執行資料安全內部稽核並提出評估報告？	□符合 □不符合 □不適用		請說明稽核之頻率及執行方式，並檢附最近一次之評估報告。
	9.2 是否採取改善措施以持續改善資料安全維護？	□符合 □不符合 □不適用		請檢附檢視或修正之紀錄，並檢附稽核矯正單及追蹤紀錄。
10. 使用紀錄、軌跡資料及證據保存	10.1 是否保存個人資料提供或移轉第三人之紀錄？	□符合 □不符合 □不適用		是否保存個人資料提供或移轉第三人之紀錄？
	10.2 是否保存當事人行使個資法第三條之權利及處理過程之紀錄？	□符合 □不符合 □不適用		請檢附當事人行使個資法第三條之權利及處理過程之紀錄。
	10.3 是否保存個人資料或儲存個人資料媒體之刪除、停止處理、利用或銷毀之原因、方法、時間及地點等紀錄？	□符合 □不符合 □不適用		請檢附個人資料或儲存個人資料媒體之刪除、停止處理、利用或銷毀之原因、方法、時間及地點等紀錄。

稽核項目	稽核內容	查核結果	說明	備註
	10.4 是否保存人員權限新增、變動及刪除之紀錄？	□符合 □不符合 □不適用		請檢附人員權限新增、變動及刪除之紀錄。
	10.5 是否保存消費者個人資料之蒐集、處理及利用紀錄，以及自動化機器設備之軌跡資料？	□符合 □不符合 □不適用		請說明留存之期限，並檢附近一年消費者個人資料之蒐集、處理及利用紀錄，以及自動化機器設備之軌跡資料。
11.個人資料安全維護之整體持續改善	11.1 是否定期就個人資料安全維護議題召開會議並提出持續改善報告？	□符合 □不符合 □不適用		請檢附相關個人資料安全維護議題會議之記錄。
	11.2 是否訂定個人資料管理(或安全維護)辦法並定期檢視更新？	□符合 □不符合 □不適用		請檢附個人資料管理(或安全維護)辦法以及完整之版本資訊，包含但不限於日期、提報人及核定人等相關資訊。。
12.委託作業	12.1 委託他人蒐集、處理或利用個人資料之全部或一部時，是否要求受託人依委託人應適用之規定為之？	□符合 □不符合 □不適用		請檢附個資委外之廠商清單及合約文件。
	12.2 委託他人蒐集、處理或利用個人資料之全部或一部時，是否於委託契約或相關文件明確約定適當	□符合 □不符合 □不適用		請檢附個資委外之廠商清單及合約文件。

稽核項目	稽核內容	查核結果	說明	備註
	之監督事項及方式？			
	12.3 委託他人蒐集、處理或利用個人資料之全部或一部時，是否確實執行監督？	□符合 □不符合 □不適用		請說明對委外廠商之監督方式或檢附委外稽核報告以及稽核缺失追蹤情形。
	12.4 是否要求受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料？	□符合 □不符合 □不適用		請檢附個資委外之廠商清單及合約文件。
	12.5 是否要求受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關？	□符合 □不符合 □不適用		請檢附個資委外之廠商清單及合約文件。
13.使用資通訊系統蒐集、處理或利用個人資料	13.1 是否就使用資通訊系統蒐集、處理或利用個人資料之服務範圍取得資安或個資驗證？	□符合 □不符合 □不適用		請檢附外部稽核證書(或驗證通過證明書)，例如 ISO 27001、27701，以確認驗證範圍包含本系統開發生命週期及對客戶提供之服務流程，以及持續有效。
14.個資存放雲端之安全控管	14.1 是否確保個人資料放在雲端上的安全？	□符合 □不符合 □不適用		請說明如何確認 Database 的安全以及放在那個國家？並提出相關佐證(如雲端業者出具的證明書)。

稽核項目	稽核內容	查核結果	說明	備註
15.發生個資事件之處理	15.1 近兩年內是否發生個人資料被竊取、洩漏、竄改或其他侵害情形之個資事件？	□符合 □不符合 □不適用		請檢附通報記錄。
	15.2 是否就個資事件委請公正之第三方進行調查？	□符合 □不符合 □不適用		請檢附就個資事件聘請第三方資安廠商就事件調查之報告。
	15.3 是否即時且適當的通知當事人？	□符合 □不符合 □不適用		請檢附向用戶說明事件緣由及防護措施之通知。
	15.4 是否就事件的發生進行根因分析，並提出強化措施？	□符合 □不符合 □不適用		請檢附事件報告、強化措施的實施情形以及相關內部會議紀錄。
16.網路零售的遵法性	16.1 如有進行網路零售之行為，是否遵循「網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法」？	□符合 □不符合 □不適用		請說明進行網路零售之網站(網址)或方式。
17.個人資料庫之共享使用	17.1 是否有其他關係企業或主體共享使用本公司所蒐集之客戶個人資料庫？	□符合 □不符合 □不適用		請說明具體共享使用之主體名稱，以及共享使用之原因及安全控管措施。另檢附告知當事人之佐證。

稽核項目	稽核內容	查核結果	說明	備註
	17.2 是否使用其他關係企業或主體所蒐集之客戶個人資料庫加以處理及利用？	□符合 □不符合 □不適用		請檢附於處理及利用前告知當事人之佐證。

附件 2 個資外洩重大矚目案件調查報告格式

[部會]個資外洩重大矚目案件調查報告

受調查非公務機關名稱
:[…]

重大矚目案件行政調查個案名稱
:[…]

報告編號：2023-部會名稱-流水號
（如：2023-xx 部-001）

日　　期：　　年　　月　　日

調查報告目錄

調查報告內文

壹、基本資訊

一、報告機關：

【負責提出或綜整提出調查報告之機關】

二、執行行政調查機關：

【依個案情形可能為單一或複數機關】

三、協助調查之機關、行政法人或團體:

三、接受行政調查非公務機關:

四、個案名稱：

【指行政調查機關就本次外洩個案設定之名稱】

貳、24 小時內監督通報過程:

一、首次知悉外洩事故之時間、方式及內容

二、符合重大矚目案件定義之說明

三、監督通報提送情形

參、3 日內開始行政調查迄今之行政作為:

一、行政調查前準備之說明:

【如：行政調查小組分工(含參與調查機關或協助者之角色)、規劃行政調查期程、與受調查非公務機關連繫情形及是否請受調查機關提供相關資料或自評等】

二、行政調查情形:

【請說明行政調查之時間、調查方式、調查範圍、調查項目、調查發現(含技術面、管理面等)、是否對廠商裁罰及提出改正要求(是否為裁罰及命改正處分)、受調查事業改正情形、後續複查等時程規劃、複查結果、是否將進行下階段處分(是否再次裁罰並命改正)…等相關事宜。若有分次調查，請按分次調查情狀，分別敘明之。】

（一）第一次…

（二）第二次…

（三）第三次…

肆、調查事實整理：

一、外洩事故機關與關連機關

【說明經調查後，本起外洩事故主體為何，若有其他關連機關(如：有受託機關、委託機關等)，請列出並說明其他關連機關於外洩事故涉及個資之角色】

二、外洩事故描述

【整理說明本次外洩事故情形，含經過、時間、事故主體與關連機關之作為等】

三、外洩事故類型分析

【屬被竊取、竄改、毀損、滅失、洩漏或為其他侵害事故】

四、受影響個人資料類別及損害評估

【一般或特種個人資料、個資內容類別描述、個資侵害筆數、詐騙金額或其他侵害情形評估】

五、非公務機關通知當事人之情形

【遵循個資法規定通知當事人之時間、方式及通知內容，若有佐證資料請一併檢附於附綠「重要參考附件」】

六、非公務機關採取應變措施

【非公務機關已採取/即將採取之應變措施，應包含技術面、管理面等，若有佐證資料請一併檢附於附錄「重要參考附件」】

伍、分析原因與處置措施

一、事故發生原因分析

【說明經調查後就事故發生原因之分析及判斷】

二、個資安全維護義務法律遵循分析

【說明事故主體及/或關聯機關是否已盡個資法第 27 條安全維護義務或符合其所應適用之個資檔案安全維護辦法或其他相關法律規範等】

三、待改善事項方案及建議作為

【管理面、技術面】

四、擬/已採取之個資法相關行政處分情形

【個資法第 25 條、第 48 條、第 49 條規定及第 50 條規定】

五、命令改正時程及查核追蹤機制

【管理面、技術面】

陸、個案調查綜合分析、建議與結論

【綜合摘要說明本案調查分析結果、建議(含對本案事故處理之建議，或對類似事件後續會如何處理之建議等)與本案調查結論等】

附錄一、調查報告摘要表

一、　基本資訊

(一)報告機關	
(二)執行行政調查機關	
(三)協助調查之機關、行政法人或團體	
(四)受調查非公務機關	
(五)個案名稱	

二、監督通報過程之簡表

知悉時間、方式及內容	符合重大矚目案件定義	監督通報提送情形

三、行政作為時序簡表

日期	行政調查或其他行政作為	取得之資料名稱	受調查非公務機關回應及態度情況

四、調查事實與應變措施

外洩事故機關與關連機關	外洩事故類型分析	受影響個人資料類型及損害評估	非公務機關通知當事人	非公務機關採取應變措施

五、分析原因與改正措施

事件發生原因分析	個資安全維護義務法律遵循分析	待改善事項方案及建議作為	採取個資法相關行政處分情形	並隨命令改正時程及查核追蹤機制

附錄二、重要參考附件