正　本

檔　　號：
保存年限：

個人資料保護委員會籌備處　公告

發文日期：中華民國115年3月9日
發文字號：個資籌查字第1150500086號
附件：如公告事項三

主旨：預告訂定「公務機關個人資料保護管理事項實施情形稽核辦法」草案。

依據：行政程序法第一百五十四條第一項。

公告事項：

一、訂定機關：個人資料保護委員會（俟該會成立後訂定發布）。

二、訂定依據：個人資料保護法第二十一條之一第五項及第二十一條之二第四項。

三、「公務機關個人資料保護管理事項實施情形稽核辦法」草案如附件。本案另登載於本籌備處全球資訊網站/最新消息（網址：https://www.pdpc.gov.tw/News/20/）、本籌備處主管法規查詢系統/草案預告（網址：https://law.pdpc.gov.tw/DraftForum.aspx）及公共政策網路參與平臺/眾開講/法令草案預告（網址：https://join.gov.tw/policies/）。

四、對於本公告內容有任何意見或修正建議者，請於本公告刊登公報次日起60日內陳述意見或洽詢：

(一)承辦單位：個人資料保護委員會籌備處

(二)地址：臺北市中正區館前路77號5樓
(三)聯絡人：陳專員
(四)電話：（02）3356-8016分機251
(五)傳真：（02）3356-8012
(六)電子郵件：mindful0519@pdpc. gov. tw

主任 李世德

裝

訂

線

公務機關個人資料保護管理事項實施情形稽核辦法草案總說明

個人資料保護法（以下簡稱本法）業於一百十四年十一月十一日修正公布，其施行日期由行政院定之。本法第二十一條之一第五項明定，公務機關督導及稽核其所屬、所監督及所轄公務機關個人資料保護管理事項實施情形之必要內容、稽核之頻率、內容與方法、結果之交付、改善報告之提出及其他相關事項之辦法，由主管機關定之；及第二十一條之二第四項明定，主管機關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之稽核頻率、內容與方法、改善報告之提出及其他相關事項之辦法，由主管機關定之。為依本法第二十一條之一及第二十一條之二規定，規範公務機關應提出個人資料保護管理事項實施情形之內容，及主管機關與上級或監督機關對所屬、所監督或所轄公務機關所進行之稽核等相關事項，以及受稽核機關後續改善相關事宜，經考量我國公務機關實務現況，訂定本辦法草案，其要點如下：

一、本辦法訂定之依據。（草案第一條）

二、本辦法重要用詞定義。（草案第二條）

三、個人資料保護管理事項實施情形之內容。（草案第三條）

四、稽核計畫之訂定。（草案第四條）

五、稽核頻率與擇定受稽核機關之考量因素。（草案第五條）

六、稽核小組之組成。（草案第六條）

七、稽核執行原則、保密義務及應主動迴避之事由。（草案第七條）

八、稽核之方式。（草案第八條）

九、稽核通知之時程、內容與稽核日期變更之申請。（草案第九條）

十、受稽核機關配合事項及無法配合之處理程序。（草案第十條）

十一、稽核報告之交付。（草案第十一條）

十二、改善報告之提出。（草案第十二條）

十三、稽核機關委請其他機關協助辦理稽核、相關配套措施及協辦機關應具備資格之規定。（草案第十三條）

十四、本辦法施行日期。（草案第十四條）

公務機關個人資料保護管理事項實施情形稽核辦法草案

條文	說明
第一條　本辦法依個人資料保護法（以下簡稱本法）第二十一條之一第五項及第二十一條之二第四項規定訂定之。	明定本辦法訂定之依據。
第二條　本辦法用詞，定義如下： 一、稽核機關：指依本法第二十一條之一第二項規定應督導及稽核其所屬、所監督或所轄公務機關個人資料保護管理事項實施情形之公務機關，及依本法第二十一條之二第一項規定應定期或不定期稽核公務機關個人資料保護管理事項實施情形之主管機關。 二、受稽核機關：指依本法第二十一條之一第一項規定應每年提出個人資料保護管理事項實施情形之公務機關。	一、本條係解釋本辦法重要用詞定義。 二、本辦法所用稽核機關及受稽核機關二詞，均有其特定涵義，爰於第一款及第二款明定。
第三條　受稽核機關應依主管機關指定方式及期限，每年提出個人資料保護管理事項實施情形，內容至少應包括下列項目： 一、機關核心業務所涉個人資料保護管理之政策及其目標。 二、依本法要求指派個人資料保護長、配置適當人力及指定專人之情形。 三、個人資料蒐集、處理及利用之內部作業流程規範。 四、個人資料保護管理所需資源之投入與配置。 五、個人資料蒐集、處理、利用與受理	一、本法規定公務機關應依據第十條、第十一條及第十三條受理當事人權利行使之請求、落實本法第十二條個人資料事故應變措施、依據本法第六條、第十五條、第十六條檢視蒐集、處理及利用個人資料之作業流程合規性、依據本法第十八條設置個人資料保護長及相關人員、執行本法第三章之一第一節對公務機關之監督，以及實施本法第十八條及個人資料檔案安全維護管理辦法之個人資料檔案安全維護事項等規定，爰參考個人資料保護實務上所採取 PDCA 循環（即 Plan 計畫

當事人權利行使等事項之辦理情形。 六、本法第十八條第二項所稱個人資料檔案安全維護事項。 七、個人資料事故之通知、通報、應變、處理、改善及統計分析。 八、內、外部稽核缺失改善情況及次年度管理機制精進規劃。 前項第三款之作業流程規範，至少應包括文件與紀錄管理、個人資料盤點與風險評估、宣導與教育訓練、委託監督、稽核及持續改善作業。	-Do 執行-Check 查核-Act 行動）之方法論，於第一項明定受稽核機關每年提出之個人資料保護管理事項實施情形之內容。 二、第二項針對前項第三款「個人資料蒐集、處理及利用之內部作業流程規範」，規範必要之文件項目。
第四條　稽核機關應每年訂定稽核計畫，並掌握稽核情形。 前項稽核計畫，其內容至少包括下列事項： 一、稽核依據。 二、稽核目的。 三、稽核範圍。 四、作業期程。 五、稽核小組組成方式。 六、受稽核機關擇定之考量因素。 七、稽核方式。 八、稽核項目及基準。	一、主管機關以外之稽核機關依據本法第二十一條之一第二項規定，應督導及稽核其所屬、所監督、所轄鄉(鎮、市)公所、直轄市山地原住民區公所及鄉(鎮、市)民代表會、直轄市山地原住民區民代表會之個人資料保護管理事項實施情形，及主管機關依據本法第二十一條之二第一項規定，應定期或不定期辦理稽核，爰配合每年提出個人資料保護管理事項實施情形之頻率，於第一項明定稽核機關應每年訂定稽核計畫、辦理稽核作業，並掌握稽核情形。 二、為利實務執行，爰於第二項明定稽核計畫基本內容事項。
第五條　主管機關以外之稽核機關應綜合考量下列因素，除因不可抗力外，每年擇定受稽核機關，稽核其個人資料保護管理事項實施情形： 一、機關業務之重要性與機敏性。	一、考量公務機關行政量能，應針對具有高風險、對於人民權益影響重大、歷年發生個人資料事故頻率、稽核結果有缺失或待改善事項之受稽核機關，優先加強稽核，以督導強化該等機關

二、保有個人資料之規模、類型。 三、蒐集、處理、利用個人資料之技術、方法。 四、個人資料保護管理之執行情形。 五、個人資料事故發生之頻率與程度。 六、受稽核機關歷年接受稽核之頻率及結果。 七、受稽核機關當年度有未依期限說明、調整改善報告或未完成改善之情事。 八、其他個人資料保護管理事項或稽核資源分配相關之事項。 主管機關應綜合考量我國個人資料保護政策、國內外個人資料保護趨勢、前項各款考量因素或其他主管機關認有必要之情形，擇定受稽核機關。 稽核機關得要求受稽核機關依第一項所列事項提出說明，作為擇定之參考。 主管機關為辦理稽核作業，得請求其他稽核機關提供必要協助。	落實個人資料保護，爰於第一項明定主管機關以外之稽核機關擇定受稽核機關時應考量之因素，以決定最適之受稽核機關。 二、為使主管機關定期或不定期稽核作業能切合我國個人資料保護政策目標，並適時反映國內外個人資料保護相關趨勢，並視稽核辦理情形合理分配稽核資源，於第二項明定主管機關機關擇定受稽核機關之應考量因素。 三、鑑於稽核機關依第一項及第二項規定擇定受稽核機關時之考量因素，與受稽核機關辦理個人資料保護管理事項之實施情形、過往接受稽核之情形及業務特性、政策目標等息息相關，有由受稽核機關或其他稽核機關提供訊息或協助之必要，爰訂定第三項及第四項規定。
第六條　稽核機關辦理稽核時，應依受稽核機關性質、組織規模、風險程度及專業需求等因素，組成適當之稽核小組。 稽核小組成員不限稽核機關人員，得依稽核需要由具備個人資料保護、資通安全、資訊、電信或法律等專長，或其他具該次稽核所需之技術、管理、實務知能之人員組成。 必要時，稽核小組得於稽核過程中洽請具所需專業之人員共同為之。	為使稽核個人資料保護管理事項實施情形得妥適辦理，爰於第一項明定稽核機關組成稽核小組應考量之相關因素。又因實務上具備稽核專業、適合擔任稽核小組成員之人員未必屬稽核機關人員，爰於第二項明定稽核小組成員不限稽核機關人員，並於第三項明訂稽核小組得洽請具當次稽核所需專業之人員共同參與稽核過程以提供專業協助。

第七條　稽核之執行應依循公正、獨立與客觀之原則。 因參與稽核而知悉或持有之相關機密資訊或文件者，應善盡保密之責。 前條第二項稽核小組成員及第三項專業人員有下列情形之一者，應主動迴避該次稽核： 一、本人、其配偶、三親等內親屬、家屬或上開人員財產信託之受託人，與受稽核機關或機關首長間有財產上或非財產上之利益關係。 二、本人、其配偶、三親等內親屬或家屬，與受稽核機關或機關首長間，目前或過去二年內有僱傭、承攬、委任、代理或其他類似之關係。 三、本人目前或過去二年內任職之機關（構）或單位，曾為稽核對象之顧問，其輔導項目與稽核項目相關。 四、其他情形足認參與該次稽核，將對稽核結果之公正性造成影響。	一、為保障受稽核機關之權益，爰於第一項明定稽核機關應依循之執行原則，及於第二項明定保密義務。 二、為確保稽核結果之客觀性及避免爭議，爰參照資通安全維護計畫實施情形稽核辦法及公職人員利益衝突迴避法相關規定，於第三項明定實際執行稽核作業並認定稽核缺失或待改善事項之稽核小組成員與共同參與稽核之專業人員應主動迴避之情形。
第八條　個人資料保護管理事項實施情形之稽核，得以實地、書面或其他適當方式為之。 稽核機關得要求受稽核機關提出管理程度自主評估或符合國際標準規範並取得財團法人全國認證基金會個人資料保護管理相關領域認證之驗證機構出具之評估報告。	為使稽核方式彈性多元以因應不同情境，爰於第一項明定稽核機關辦理稽核作業方式得以實地、書面或視訊等其他適當方式，並於第二項明定稽核機關得要求受稽核機關提出相關評估報告，作為稽核之參考資料。
第九條　稽核機關辦理稽核時，應於一個月前以書面通知受稽核機關。但稽核機關依本條第五項第一款或第十條第三項第二款擇期辦理之稽核，或主管機關依	一、為利受稽核機關有適當時間預為準備，以配合辦理稽核業務，爰於第一項明定稽核機關以書面通知受稽核機關之期限。

本法第二十一條之二第一項辦理之不定期稽核，得於十個工作日前通知受稽核機關。 前項稽核通知之內容，應包括預計稽核期間、稽核範圍、稽核重點、稽核方式、受稽核機關或其他機關配合或協助事項及其他必要事宜。 受稽核機關於接獲稽核通知後，應依稽核機關之要求，於期限內依稽核重點提出說明及相關佐證資料，並配合稽核機關安排之訪談。 受稽核機關如因業務因素或其他正當理由，未能為前項配合或提交者，得於收受前項通知後五個工作日內，以書面敘明理由向稽核機關申請變更稽核日期或為其他適當之處理。 稽核機關收受前項書面後，應進行審核，並依下列規定辦理： 一、認有理由者，應將審核之依據及相關資訊記載於稽核報告，並得擇期辦理稽核作業或為其他適當之處理。 二、認無理由者，應要求受稽核機關依第三項規定辦理。 第四項申請除有不可歸責之事由，以一次為限。	二、為使稽核過程遂行，於第二項明定稽核通知內容應包括稽核過程預計所需時間、稽核範圍、稽核重點、稽核方式、受稽核機關聯繫或陪同人員之指派、稽核場地與設備之安排、業務相關機關或委外廠商之必要協助等事項，並於第三項明定受稽核機關於稽核作業開始前，應依稽核機關所定期限，提出說明與佐證資料並配合訪談，以為準備。 三、考量受稽核機關可能有因業務因素或其他正當理由，難以依稽核機關所定日期或要求配合稽核準備之情形，爰於第四項明定於此情形，受稽核機關得於收受第一項通知後，於規定期限內以書面敘明理由向稽核機關申請調整稽核日期或為其他適當之處理，並於第五項明定稽核機關受理申請後之審核規定。另於第六項明定其申請除有不可歸責之事由外，以一次為限。
第十條　稽核機關於稽核過程，得要求受稽核機關針對個人資料保護管理事項實施情形提出補充說明、提供相關文件、證明資料供稽核小組查閱或為其他協助，受稽核機關及其所屬人員應予配合。 受稽核機關依法律有正當理由，未	一、為利主管機關藉由稽核作業確認受稽核機關遵循本法之情形，爰於第一項明定稽核機關於稽核時，得要求受稽核機關配合之事項。 二、受稽核機關如依法律有正當理由，不能為第一項之配合事項，例如法律明

能為前項說明、提出資料供查閱或協助者，應以書面敘明理由，向稽核機關提出。 稽核機關收受前項書面後，應進行審核，依下列規定辦理： 一、認有理由者，應將審核之依據及相關資訊記載於稽核報告，並得停止稽核作業之全部或一部。 二、認無理由者，應要求受稽核機關依第一項規定辦理；因審核程序而停止稽核作業者，得擇期續行辦理。	定列為國家機密、應予保密或不得提供之資料，此時受稽核機關應以書面敘明其理由，向稽核機關提出，俾利稽核機關審核及決定是否繼續該項作業，爰為第二項及第三項規定。另受稽核機關依第二項提出申請，經稽核機關認無理由且致影響稽核執行或結果之認定者，稽核機關得據以認定為缺失或待改善事項，併予敘明。
第十一條　稽核機關應於第九條第二項所定稽核期間結束後三個月內，將稽核報告交付受稽核機關。因故未能交付者，應將未能交付稽核報告之事由告知受稽核機關。 前項稽核報告內容應包括： 一、稽核對象基本資料與稽核日期。 二、稽核範圍、稽核方式及過程摘要。 三、未能為說明、協力或提出資料供稽核小組查閱之情形、理由與處理結果。 四、第九條第五項及第十條第三項所定稽核機關審查結果。 五、稽核缺失或待改善事項。 六、改善提出方式與期限。 七、其他與稽核相關之必要內容。 受稽核機關對稽核報告內容有異議時，應於報告送達之次日起十個工作日內，以書面敘明理由向稽核機關提出。稽核機關認為有理由者，得修正稽核報告內容。	為利受稽核機關得依稽核結果進行改善，爰明定稽核機關交付稽核報告之時限，及稽核報告應記載之內容。

第十二條　受稽核機關經稽核發現其個人資料保護管理事項實施情形有缺失或待改善者，應於稽核報告送達後，依稽核機關指定方式及期限，提出包括下列項目之改善報告及其執行情形，送交依本法第二十一條之一第一項規定收受其實施情形之機關審查後，由該審查機關送交主管機關： 一、稽核缺失或待改善之項目與內容。 二、發生原因。 三、為改正缺失或補強待改善項目所採取技術上及組織上之措施。 四、預定完成時程與執行進度之追蹤方式。 前項審查機關或主管機關認有必要時，得要求受稽核機關進行說明或調整。 第一項改善報告，受稽核機關應保存五年。	一、依據本法第二十一條之一第三項及第二十一條之二第二項規定，受稽核機關經發現其個人資料保護管理事項實施情形有缺失或待改善事項者，應向法定機關提出改善報告。為利法定機關追蹤管考確認，爰於第一項明定受稽核機關應提出改善報告之期限及改善報告之內容。 二、為落實公務機關層級監督及主管機關外部監督之效，爰於第二項明定本法第二十一條之一第一項規定收受實施情形之機關及主管機關均得要求受稽核機關進行說明或調整改善報告。 三、為有效執行個人資料保護之 PDCA 循環，避免相同缺失重複發生或待改善事項未落實改善，爰於第三項明定受稽核機關應保存改善報告五年，俾憑稽核機關辦理下次稽核作業時之參考資料。
第十三條　稽核機關得委請其他機關(構)、行政法人或公益團體協助辦理稽核相關事務，並應以書面約定辦理事務範圍、人員資格、保密義務、稽核權限、執行報告、內部控制機制、監督配合等必要事項，並進行督導考評。 前項協助辦理稽核相關事務之機關(構)、行政法人或公益團體應具備充足之專業人員、技術能力與實務經驗，及健全之內部控制與保密機制。	考量稽核作業之專業性，爰於第一項明定稽核機關得委請其他機關(構)、行政法人或公益團體協助辦理稽核相關事務及其必要之督導考評事項，並於第二項明定稽核機關委請協助辦理前，須逐項審酌確認其他機關(構)、行政法人或公益團體應具備之條件。
第十四條　本辦法施行日期，由主管機關定之。	配合本法修正期程，明定施行日期由主管機關定之。