交通部　公告　　中華民國 113 年 7 月 3 日
交授象綜字第 11300539431 號

主　　旨：預告訂定「交通部指定氣象產業類非公務機關個人資料檔案安全維護計畫及處理辦法」。

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：交通部。

二、訂定依據：個人資料保護法第二十七條第三項。

三、「交通部指定氣象產業類非公務機關個人資料檔案安全維護計畫及處理辦法」草案如附件。本案另載於本部中央氣象署全球資訊網站／資料／政府資訊主動公開／法案公告網頁（網址：https://www.cwa.gov.tw）及「公共政策網路參與平台」之「眾開講」（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隔日起 60 日內陳述意見或洽詢：

（一）承辦單位：中央氣象署

（二）地址：臺北市中正區公園路 64 號

（三）聯絡人：吳技正

（四）電話：02-23491018

（五）傳真：02-23491019

（六）電子郵件：wesley@cwa.gov.tw

交通部指定氣象產業類非公務機關個人資料檔案安全維護計畫及處理辦法草案總說明

依個人資料保護法(以下簡稱本法)第二十七條第一項規定，非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏；同條第二項及第三項規定，中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法，其相關事項之辦法，由中央目的事業主管機關定之。為使相關非公務機關自行或受委託蒐集、處理或利用個人資料檔案，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏，爰依上開規定訂定交通部指定氣象產業類非公務機關個人資料檔案安全維護計畫及處理辦法（以下簡稱本辦法），以資遵循；本辦法共計二十二條，其要點如下：

一、本辦法訂定依據、適用對象及名詞定義。（草案第一條、第二條）

二、非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法內容與時限。（草案第三條、第四條）

三、非公務機關配置適當管理人員落實執行計畫及處理方法等事項。（草案第五條）

四、保有個人資料特定目的之界定及個人資料檔案現況之盤點、業務流程之風險分析與管控，及相關侵害事故之應變等事項。（草案第六條至第八條）

五、非公務機關所屬人員為執行業務蒐集個人資料之規範、非公務機關所蒐集持有及應遵守告知義務等事項。（草案第九條、第十條）

六、非公務機關委託他人蒐集、處理或利用個人資料時，應對受託者為適當之監督。（草案第十一條）

七、非公務機關國際傳輸個人資料時應遵循事項。（草案第十二條）

八、非公務機關對於當事人行使本法第三條規定權利時應採取之措施。（草案第十三條）

九、非公務機關對所保管之個人資料檔案所應採取之必要適當防護設施，及對所屬人員之管理措施。（草案第十四條、第十五條）

十、非公務機關使用資通訊系統蒐集、處理或利用個人資料時應採取之

資通訊安全措施。（草案第十六條）

十一、非公務機關對所屬人員進行教育宣導規定。（草案第十七條）

十二、計畫及處理方法之稽核、使用紀錄留存及檢討改善事項。（草案第十八至二十條）

十三、非公務機關業務終止後所保有個人資料之處理方式。（草案第二十一條）

十四、本辦法施行日期。（草案第二十二條）

交通部指定氣象產業類非公務機關個人資料檔案安全維護計畫及處理辦法草案

條　文	說　明
第一條　本辦法依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定之。	一、本辦法之訂定依據。 二、本法第二十七條第二項：「中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。」及同條第三項：「前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。」
第二條　本辦法所稱非公務機關，包括下列各款： 一、氣象預報業。 二、海象預報業。 三、氣象及海象預報業。 本辦法所稱主管機關為交通部。	第一項明定本辦法之適用對象，其所稱之非公務機關，指依氣象法第十八條規定經交通部中央氣象署許可，從事氣象預報業、海象預報業、氣象及海象預報業之團體。
第三條　非公務機關應訂定個人資料檔案安全維護計畫及業務終止後個人資料處理方法（以下簡稱安全維護計畫），以落實個人資料檔案之安全維護與管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 非公務機關應依其所訂定之安全維護計畫執行之。交通部中央氣象署（以下簡稱本署）得要求非公務機關提出安全維護計畫之實施情形，非公務機關應於指定期限內，以書面方式提出。	一、第一項依本法第二十七條第二項規定，明定非公務機關應訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法，規範非公務機關落實個人資料檔案之安全維護與管理措施。安全維護計畫訂定後，應依第二十條規定定期檢視或修正。 二、非公務機關依第一項訂定安全維護計畫後，應據以執行。依本法第二十二條規定，主管機關為執行檢查，得要求非公務機關提出安全維護計畫實施情形，爰於第二項規定非公務機關提出實施情形之期限及方式。
第四條　非公務機關依前條規定訂定安全維護計畫時，應視其組織規模、特性、保有個人資料之性質及數量等事項，參酌第五條至第二十條規定，訂定包含下列事項之個人資料檔案之安全管理措施： 一、非公務機關之組織規模及特性。 二、個人資料檔案之安全管理措	考量非公務機關大小規模差異，組織型態不盡相同，尚難作統一規範，爰規定非公務機關得參酌其組織規模、特性、保有個人資料之性質及數量等事項，參考第五條至第二十條及本法施行細則第十二條第二項規定，訂定適宜並符合比例原則之安全措施，據以執行。

施： （一）配置管理之人員及相當資源。 （二）界定蒐集、處理及利用個人資料之範圍。 （三）個人資料之風險評估及管理機制。 （四）事故之預防、通報及應變機制。 （五）個人資料蒐集、處理及利用之內部管理程序。 （六）設備安全管理、資料安全管理及人員管理措施。 （七）認知宣導及教育訓練。 （八）資料安全稽核機制。 （九）使用紀錄、軌跡資料及證據保存。 （十）個人資料安全維護之整體持續改善。 （十一）業務終止後之個人資料處理方法。	
第五條　非公務機關就個人資料檔案之安全維護管理，得指定專人或專責組織負責，並配置相當之資源。 安全維護計畫之訂定或修正，應經非公務機關代表人或經其授權之人員核定。 個人資料檔案安全維護管理組織，應定期就執行任務情形向非公務機關代表人或經其授權之人員提出書面報告。 非公務機關應將訂定之安全維護計畫留存於營業所在地備查；主管機關得派員檢查。	一、為有效訂定與執行維護計畫，明定非公務機關就個人資料檔案安全維護管理得指定專人或建立專責組織，並配置相當資源及專人或專責組織之任務，以確保個人資料維護安全措施發揮效能。 二、本法第四十八條第二、三項及第五十條規定，對違反本法第二十七條第一項或未依同條第二項訂定計畫及處理方法者，併同處罰非公務機關及其代表人，爰第二項規定本計畫及處理方法應經非公務機關代表人或經其授權之人員核定。 三、第三項規定負責計畫及處理方法之管理人員須定期向負責人提出報告，促使負責人能據以監督計畫及處理方法之執行，落實對個人資料保護之工作。 四、第四項規定非公務機關應將其安全維護計畫留存營業處所備查。
第六條　非公務機關應依個人資料保	本條規定個人資料特定目的之界定及

護相關法令，定期查核確認所保有之個人資料現況，界定其納入本計畫及處理方法之範圍。	個人資料檔案現況之定期盤點。
第七條　非公務機關應依前條界定之個人資料範圍及其蒐集、處理、利用個人資料之流程，評估可能產生之個人資料風險，並根據風險評估之結果，訂定適當之管控機制。	本條規定非公務機關業務流程之風險分析與管控事項。
第八條　非公務機關為因應保有個人資料被竊取、竄改、毀損、滅失或洩漏等安全事故，應訂定採取下列事項： 一、適當之應變措施，以控制事故對當事人之損害。 二、查明事故之狀況並以適當方式通知當事人；其通知內容包含個人資料發生事故之事實、非公務機關所採取之因應措施及所提供之諮詢服務專線。 三、研訂預防機制，避免類似事故再次發生。 非公務機關應於發現前項事故後七十二小時內填具個人資料侵害事故通報及紀錄表，通報本署；未於時限內通報者，應附延遲理由（通報格式如附表）。 前項事故通報後，主管機關得依本法第二十二條至第二十六條規定所賦予之職權，為適當之監督管理措施。	一、配合本法施行細則第十二條第二項第四款，為降低或控制因個人資料被竊取、竄改、毀損、滅失或洩漏等事故造成主體財產及非財產之損害，非公務機關應訂定個人資料安全事故應變、通報及預防機制。 二、第二項參酌民用航空事業個人資料檔案安全維護計畫及處理辦法第六條規定，並依行政院及所屬各機關落實個人資料保護聯繫作業要點第四點第一項第三款有關個資外洩時應通報之對象、時點、應通報事項、後續行政檢查等事項訂定。 三、另因應個人資料侵害事故發生，主管機關於接獲通報後，得依本法第二十二條至第二十六條所規範為適當之監督管理措施，相關監督管理措施並得依同法第五十二條第一項規定委任本署辦理。
第九條　非公務機關所屬人員為執行業務而蒐集、處理一般個人資料時，應檢視是否符合本法第十九條之要件；利用時，應檢視是否符合蒐集之特定目的必要範圍；為特定目的外之利用時，應檢視是否符合本法第二十條第一項但書情形。	本條揭示非公務機關所屬人員執行業務蒐集、處理、利用一般個人資料時，應遵守相關法定要件及程序。
第十條　非公務機關蒐集個人資料，應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求所屬人員確實辦理。	為尊重當事人能知曉其個人資料被蒐集、處理及利用之狀況，本法第八條及第九條規定資料蒐集者有告知義務，爰規定非公務機關，應區分個人資料蒐集方式，分別訂定告知之方法、內容及相關注意事項，以便所屬人員據以執行。

第十一條　非公務機關委託他人蒐集、處理或利用個人資料之全部或一部時，應依本法施行細則第八條規定為適當監督。 　　非公務機關為執行前項監督，應與受託者明確約定相關監督事項及方式。	依本法施行細則第八條之規定，委託他人蒐集、處理或利用個人資料時，委託者應為適當之監督，避免受託者有違反本法情事發生，爰明定非公務機關委託他人蒐集、處理或利用個人資料時，應為適當之監督，並與受託者約定相關監督事項與方式。
第十二條　主管機關依本法第二十一條規定，對非公務機關為限制國際傳輸個人資料之命令或處分時，非公務機關應通知所屬人員遵循辦理。 　　非公務機關將個人資料作國際傳輸者，應檢視是否受主管機關限制，並告知當事人其個人資料所欲國際傳輸之區域，且對資料接收方為下列事項之監督： 一、預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。 二、當事人行使本法第三條所定權利之相關事項。	一、第一項依本法第二十一條規定主管機關所為之命令或處分，非公務機關應通知所屬人員知曉並遵照辦理。 二、第二項規定非公務機關將個人資料作國際傳輸者，應檢視是否受主管機關依本法第二十一條規定之命令或處分限制，並且告知個人資料所欲國際傳輸之區域，同時對資料接收方為相關之監督。
第十三條　非公務機關於個人資料當事人行使本法第三條規定之權利時，應依下列規定辦理： 一、提供聯絡窗口及聯絡方式。 二、確認為個人資料當事人本人，或經其委託者。 三、認有本法第十條但書各款、第十一條第二項但書或第三項但書規定得拒絕當事人行使權利之事由時，應附理由通知當事人。 四、有收取必要成本費用者，應告知當事人收費基準。 五、遵守本法第十三條有關處理期限之規定。	依本法第三條規定，當事人就其個人資料得行使查詢或請求閱覽、製給複製本、補充或更正、停止蒐集、處理或利用及刪除其個人資料等權利，且非公務機關除依本法第十條但書、第十一條第二項但書或第三項但書規定得拒絕當事人行使權利之情形外，應依當事人之請求辦理，並應於本法第十三條規定期間內准駁，爰明定非公務機關應遵循辦理事項，以利資料當事人行使權利。
第十四條　非公務機關對所蒐集保管之個人資料檔案，應採取必要適當之安全設備或防護措施。 　　前項安全設備或防護措施，應包含下列事項： 一、紙本資料檔案之安全保護設施。	一、為確保非公務機關所保管之個人資料檔案不被竊取、竄改、毀損、滅失或洩漏，爰規定非公務機關得視其規模、業務性質、資料儲存之媒介物及其數量等，於所訂計畫及處理方法中採取必要且適當之安全設備或防護措施。

二、電子資料檔案及資料庫存放之電腦、自動化機器相關設備、可攜式設備或儲存媒體，配置安全防護系統或加密機制。 三、存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片或其他存放媒介物報廢汰換或轉作其他用途時，應採取適當之銷毀或防範措施，避免洩漏個人資料；委託他人執行者，非公務機關對受託者之監督依第十一條規定辦理。	二、儲存個人資料之媒介物（參考政府資訊公開法第三條規定之立法例），嗣報廢或轉作其他用途時（例如：移轉與他人），採適當防範措施，以免由該媒介物洩漏個人資料（例如：燒毀、裁碎、磁性媒體予以消磁或破壞、回收再利用之紙本不含個人資料之記載部分等）。另倘委託第三者執行報廢或轉作其他用途時，對受委託者之監督依第十一條有關監督規定辦理。
第十五條　非公務機關為確實保護個人資料之安全，應對其所屬人員採取適度管理措施。 前項管理措施，應包含下列事項： 一、依據業務需求，適度設定所屬人員不同之權限，控管其接觸個人資料之情形，並定期檢視權限內容之適當性及必要性。 二、檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。 三、要求所屬人員妥善保管個人資料之儲存媒介物，並約定保管及保密義務。 四、所屬人員異動或離職時，應將執行業務所持有之個人資料辦理交接，不得在外繼續使用，並應簽訂保密切結書。	一、 非公務機關及所屬人員均應避免個人資料之保管及處理發生弊端，導致侵害當事人權益情事，爰第一項規定應於計畫及處理方法中對所屬人員採取必要且適當之管理措施。 二、 第二項規定非公務機關應根據業務性質，檢視容易發生問題之處，預先予以防範。例如：授予必要利用個人資料人員不同等級之權限、所屬人員在個人資料蒐集、處理及利用流程中有無漏洞、約束規範嚴密保管個人資料檔案及所屬人員離職時，所持有之個人資料如何交接與保密切結等事項。
第十六條　非公務機關使用資通訊系統蒐集、處理或利用個人資料者，為維護所保有個人資料之安全，應採取下列資料安全管理措施： 一、使用者身分確認及保護機制。 二、個人資料顯示之隱碼機制。 三、網際網路傳輸之安全加密機制。 四、個人資料檔案及資料庫之存取控制與保護監控機制。 五、防止外部網路入侵對策。 六、非法或異常使用行為之監控與因應機制。	非公務機關應採取之資料安全管理措施。

第十七條　非公務機關應定期或不定期對於所屬人員施以基礎個人資料保護認知宣導及教育訓練，使其明瞭相關法令之要求、所屬人員之責任範圍與各種個人資料保護事項之機制、程序及措施。	非公務機關應定期或不定期對所屬人員施以認知宣導或教育訓練，以使所屬人員能充分認知個人資料保護相關法令及責任範圍，避免發生違法情事。
第十八條　非公務機關應訂定個人資料安全稽核機制，定期或不定期查察是否落實執行所訂之安全維護計畫等相關事項。	非公務機關應訂定個人資料安全稽核機制，查察是否落實執行所訂之維護計畫或業務終止後個人資料處理方法等相關事項。
第十九條　非公務機關執行安全維護計畫所定各種個人資料保護機制、程序及措施，應記錄其個人資料使用情況，留存軌跡資料或相關證據。 非公務機關依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄： 一、刪除、停止處理或利用之方法、時間或地點。 二、將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間、地點，及該對象蒐集、處理或利用之合法依據。 前二項之軌跡資料、相關證據及紀錄，應至少留存五年。但法令另有規定或契約另有約定者，不在此限。	非公務機關應記錄其個人資料使用情況，並留存軌跡資料或相關證據；另於依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料時，亦應留存相關紀錄；且上述軌跡資料、相關證據及紀錄，除法令另有規定或契約另有約定者外，應至少留存五年。
第二十條　非公務機關應隨時參酌業務與安全維護計畫之執行狀況、社會輿情、技術發展及相關法規增修等因素，檢討所定安全維護計畫，必要時予以修正。	考量科技發展進步，社會活動型態亦隨之改變，爰明定非公務機關應注意媒體對個人資料侵害、保護事件相關報導及個人資料保護法令增修情形，隨時檢討所訂計畫，如有不合時宜之處，應立即修正，以落實保護個人資料。
第二十一條　非公務機關業務終止後，其保有之個人資料不得繼續使用，應依下列方式處理，並留存相關紀錄，其保存期限至少五年： 一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。 二、移轉：移轉之原因、對象、方	一、非公務機關因解散、歇業、公司合併或其他原因終止業務後，自不得再繼續持有使用個人資料，應作妥善處置。爰明定終止業務之非公務機關，應將所保有之個人資料予以銷毀、移轉或其他刪除、停止處理或利用等方式處

法、時間、地點及受移轉對象得保有該項個人資料之合法依據。 三、其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。	理。 二、非公務機關在銷毀、移轉或其他刪除、停止處理或利用個人資料過程中，宜保存執行方法、時間、地點、執行人員、接受移轉個人資料之對象及合法移轉個人資料之法規依據等資料，以便日後舉證。
第二十二條　本辦法自發布日施行。	本辦法施行日期。

第八條附表

<table>
<tr><td colspan="3">個人資料侵害事故通報及紀錄表</td></tr>
<tr><td>公司名稱

通報機關</td><td colspan="2">通報時間： 年 月 日 時 分
通報人： 簽名(蓋章)
職稱：
電話：
Email：
地址：</td></tr>
<tr><td>發生時間</td><td colspan="2">中華民國 年 月 日 時 分</td></tr>
<tr><td rowspan="2">發生種類</td><td rowspan="2">□竊取
□竄改
□毀損
□滅失
□洩漏
□其他侵害情形</td><td>個人資料侵害之總筆數(大約)</td></tr>
<tr><td>□一般個人資料___筆
□特種個人資料___筆</td></tr>
<tr><td>發生原因及摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個人資料侵害可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於發現個人資料外洩後七十二小時內通報</td><td colspan="2">□是
□否，理由：</td></tr>
</table>

備註：特種個人資料，指有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料；一般個人資料，指特種個人資料以外之個人資料。