

交通部民用航空局 函

地址：105008臺北市松山區敦化北路340號
傳真：02-2349-6050
聯絡人：李紀樺
電話：02-2349-6047
電子信箱：chli0918@mail.caa.gov.tw

受文者：台北市航空貨運承攬商業同業公會

發文日期：中華民國115年2月2日
發文字號：空運管字第1151500370號
速別：普通件
密等及解密條件或保密期限：
附件：如主旨 (1151500370-0-0.pdf)

主旨：函轉個人資料保護委員會籌備處檢送有關公告預告訂定「個人資料事故通知通報及應變辦法」、「個人資料檔案安全維護管理辦法」，及修正「個人資料保護法施行細則」等草案，請查照。

說明：

- 一、依據交通部115年1月23日交科字第1150002621號函、同年月日交科字第1150002623號函暨同年月日交科字第1150002624號函辦理。
- 二、旨揭草案同時登載於該籌備處全球資訊網站/最新消息(網址：<https://www.pdpc.gov.tw/News/20/>)、該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台/眾開講/法令草案預告(網站：<https://join.gov.tw/policies/>)。
- 三、對於旨揭公告內容有任何相關意見或修正建議，請於預告期間內向該籌備處或於說明二之平台提出。

正本：中華航空股份有限公司、長榮航空股份有限公司、星宇航空股份有限公司、台灣



虎航股份有限公司、立榮航空股份有限公司、華信航空股份有限公司、德安航空股份有限公司、台北市航空運輸商業同業公會、臺灣地區航空公司代表協會、台北市航空貨運承攬商業同業公會、高雄市航空貨運承攬商業同業公會、中華民國航空貨物集散站經營商業同業公會

副本：



裝

訂

線



檔 號：
保存年限：

交通部 函

地址：100299臺北市仁愛路1段50號
傳真：(02)2382-0655
聯絡人：施先生
電話：(02)2349-2838

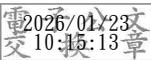
受文者：交通部民用航空局

發文日期：中華民國115年1月23日
發文字號：交科字第1150002624號
速別：普通件
密等及解密條件或保密期限：
附件：如文(1150002624-0-0.pdf、1150002624-0-1.PDF)

主旨：函轉個人資料保護委員會籌備處檢送115年1月22日個資籌
查字第1140500549號公告影本1份，請查照。

說明：依據個人資料保護委員會籌備處115年1月22日個資籌查字
第1140500549B號函辦理。

正本：部內各單位、部屬各機關(構)

副本：

裝

訂

線

檔 號：

保存年限：

個人資料保護委員會籌備處 函

地址：100011臺北市中正區館前路77號5樓

承辦人：黃守儀

電話：(02)3356-8016分機256

傳真：(02)3356-8012

電子信箱：sony@pdpc.gov.tw

受文者：交通部

發文日期：中華民國115年1月22日

發文字號：個資籌查字第1140500549B號

速別：普通件

密等及解密條件或保密期限：

附件：如主旨(公告稿pdf檔-含總說明及逐條說明.pdf)

主旨：檢送本籌備處115年1月22日個資籌查字第1140500549號公告影本1份。

正本：總統府、國家安全會議、行政院、立法院、司法院、考試院、監察院、內政部、外交部、國防部、財政部、教育部、法務部、經濟部、交通部、勞動部、衛生福利部、農業部、文化部、環境部、數位發展部、國家科學及技術委員會、國家發展委員會、大陸委員會、金融監督管理委員會、海洋委員會、僑務委員會、國軍退除役官兵輔導委員會、原住民族委員會、客家委員會、行政院公共工程委員會、行政院主計總處、行政院人事行政總處、中央銀行、國立故宮博物院、中央選舉委員會、公平交易委員會、國家通訊傳播委員會、運動部、國家運輸安全調查委員會、不當黨產處理委員會、核能安全委員會、各直轄市及各縣(市)政府、各直轄市議會及各縣(市)議會

副本：

2026/01/22
09:27:10
電子印章

裝

訂

線

個人資料保護委員會籌備處 公告

發文日期：中華民國115年1月22日
發文字號：個資籌查字第1140500549號
附件：如公告事項三



主旨：預告訂定「個人資料事故通知通報及應變辦法」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：個人資料保護法第十二條第四項。
- 三、「個人資料事故通知通報及應變辦法」草案如附件。本案另登載於本籌備處網站（網址：<https://www.pdpc.gov.tw/>）「最新消息」項下網頁、本籌備處「主管法規查詢系統」網站（網址：<https://law.pdpc.gov.tw/>）「草案預告」項下網頁及「公共政策網路參與平台」網站之「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：黃視察。
 - （四）電話：(02)3356-8016分機256、205。
 - （五）傳真：(02)3356-8012。



(六) 電子郵件：sony@pdpc.gov.tw。

(七) 「公共政策網路參與平臺」之「眾開講」。

主任

李世德



裝

訂

線

個人資料事故通知通報及應變辦法草案總說明

「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。本法第十二條第四項明定，公務機關或非公務機關知悉所保有之個人資料被竊取、竄改、毀損、滅失或洩漏（以下簡稱個資事故）時，應通知或通報之內容、方式、時限與通報範圍、應變措施、紀錄保存及其他相關事項之辦法，由主管機關定之。為使公務機關或非公務機關於知悉個資事故時適時通知當事人、通報主管機關及採取即時有效之應變措施，俾使當事人得自主維護其權益、使主管機關掌握事態並按其影響程度進行適切之調查及協助，避免損害擴大、強化個資事故之監管，爰依前開規定訂定「個人資料事故通知通報及應變辦法」（以下簡稱本辦法）草案，其要點如下：

- 一、本辦法訂定之依據。（草案第一條）
- 二、個資事故通知當事人時限、方式及內容。（草案第二條）
- 三、個資事故通報時限、方式、範圍及內容。（草案第三條）
- 四、知悉個資事故後應採取之應變措施。（草案第四條）
- 五、委託關係之知悉時點。（草案第五條）
- 六、個資事故調查紀錄之應記載事項及保存期限。（草案第六條）
- 七、本辦法之施行日期。（草案第七條）

個人資料事故通知通報及應變辦法草案

條文	說明
<p>第一條 本辦法依個人資料保護法（以下簡稱本法）第十二條第四項規定訂定之。</p>	<p>明定本辦法訂定之依據。</p>
<p>第二條 公務機關或非公務機關（以下簡稱事故機關）知悉所保有之個人資料被竊取、竄改、毀損、滅失或洩漏（以下簡稱個資事故），應於知悉時起七十二小時內以適當方式個別通知當事人。但有下列情形之一者，事故機關得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之，並應至少連續公開三十日：</p> <p>一、未有個資事故所涉當事人之聯絡方式、聯絡方式有遺失或無法辨識之情事，致無法以適當方式個別通知當事人。</p> <p>二、該個資事故未涉有本法第六條第一項所規定之個人資料，且該個人資料已經採取適當保護措施，致未經授權者無法讀取其內容。</p> <p>三、所採個別通知當事人之方式需費過鉅，將影響事故機關之營運。</p> <p>前項通知內容應包括下列事項：</p> <p>一、發生個資事故時間及事實。</p> <p>二、受影響之個人資料類別。</p> <p>三、依第四條規定採取之應變措施。</p> <p>四、事故機關聯絡方式、救濟或諮詢管道。</p>	<p>一、為使當事人儘速知悉個資事故，俾其有所警覺後，得自主評估、關注可能之權益損害，避免損害擴大，同時為利事故機關辦理通知之事項明確、一致，參考南韓個人資料保護法第三十四條、該法施行令第三十九條、日本個人資料保護法第二十六條及該法施行規則第九條規定，於第一項明定事故機關知悉個資事故後，應於七十二小時內以適當方式個別通知當事人。另符合特定情形時，事故機關得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之，例如事故機關若主張本條第一項第三款事由，應釋明個別通知當事人具體金額之計算方式，以及該金額何以影響營運之說明。</p> <p>二、為利當事人得以確切掌握個資事故情形，以採取適當作為，保障其權益，爰於第二項明定通知內容應包括事項。</p> <p>三、為使當事人得儘速知悉個資事故，於第三項明定事故機關通知當事人之適當方式。</p> <p>四、考量個資事故樣態多元，爰於第四項明定事故機關倘未能於知悉起七</p>

<p>第一項所稱適當方式，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式。</p> <p>事故機關有正當事由未能於第一項所定期限內通知當事人者，應敘明具體事由送本法第十二條第二項受理通報之機關，並應於未能如期通知之事由消滅後七十二小時內依第一項規定補行通知。</p>	<p>十二小時內通知當事人者，應敘明具體事由送本法第十二條第二項受理通報之機關，惟仍應於未能如期通知之事由消滅後七十二小時內依第一項規定補行通知，以保障當事人權益。</p>
<p>第三條 個資事故屬下列通報範圍之一者，事故機關應於知悉時起七十二小時內依主管機關指定之方式向本法第十二條第二項所定機關辦理個資事故之通報：</p> <ol style="list-style-type: none"> 一、涉有本法第六條第一項所規定之個人資料。 二、所涉之資通系統保有個人資料筆數達一萬筆以上。 三、所影響之個人資料筆數達一百筆以上。 <p>前項通報內容應包括下列項目：</p> <ol style="list-style-type: none"> 一、個資事故機關名稱。 二、個資事故發生時間及地點。 三、事故機關知悉個資事故時間及來源。 四、個資事故發生原因及類型。 五、個資事故所涉個人資料類別、估計數量及損害狀況。 六、依第二條規定通知當事人之方式及內容。 七、依第四條規定採取之應變措施。 	<ol style="list-style-type: none"> 一、為落實我國個人資料保護，參考南韓個人資料保護法第三十四條、該法施行令第四十條、日本個人資料保護法第二十六條、該法施行規則第七條、第八條及第四十三條規定，於第一項明定事故機關辦理個資事故通報之範圍。事故機關知悉屬應通報範圍者，應於知悉時起七十二小時內依主管機關指定之方式及對象辦理通報。又知悉起算點係以事故機關知悉個資事故且該個資事故符合第一項各款通報範圍時，開始起算七十二小時。另個人資料筆數之計算，比照個人資料檔案安全維護管理辦法第四條第一項規定，以非公務機關或公務機關單日所保有每一自然人之每一蒐集特定目的加總計算。 二、為強化個資事故之管理、追蹤及加速處理之效率，於第二項明定事故機關辦理個資事故通報作業之基本通報項目。

<p>八、其他相關事項。</p> <p>事故機關因故無法依第一項所定主管機關指定方式通報者，應於同項所定時間內依其他適當方式通報，並註記無法依主管機關指定方式通報之事由。</p> <p>因天災、事變或其他不可抗力之事由，致事故機關不能於第一項所定期間內通報者，應於妨礙事由消滅後四十八小時內向本法第十二條第二項所定機關補行通報，並註記無法於第一項所定期間內通報之事由。</p>	<p>三、事故機關辦理通報時，倘發生無法依主管機關指定之方式進行個資事故通報之情事，例如事故機關所在地發生網路或電力中斷，致無法向主管機關所指定之個資事故通報網站辦理通報等情事，爰於第三項明定因故無法依指定方式通報時，事故機關應依其他適當方式進行通報，並註記說明阻礙通報之事由。</p> <p>四、考量事故機關遇有天災、事變等情況危急之不可抗力事由，無法於第一項所定期間內通報個資事故時，為保護其生命、財產安全，同時兼顧個資事故之管理，爰於第四項明定事故機關仍應於妨礙事由消滅後四十八小時內補行通報。</p>
<p>第四條 事故機關知悉個資事故後，應採取下列即時有效之應變措施：</p> <p>一、檢查洩漏途徑，並採取隔離或封鎖措施。</p> <p>二、檢查存取權限，阻止異常存取路徑。</p> <p>三、收回誤送之個人資料檔案；要求第三人刪除或銷毀誤送之個人資料檔案。</p> <p>四、請求搜尋引擎業者刪除已公開之個人資料，或為消除該等個人資料公開狀態之措施。</p> <p>五、其他即時有效防止個資事故擴大之措施。</p> <p>事故機關辦理前項應變措施，應綜合考量個資事故之發生原因、受影</p>	<p>一、為保障個人資料當事人權益，避免個資事故可能產生之損害擴大，參考南韓個人資料保護法第三十四條規定及南韓個人資料委員會發布之個人資料外洩等事故應對手冊內容，於第一項明定事故機關於知悉個資事故後，應採取即時有效之應變措施。另隨著科技進步，駭客攻擊手法日新月異，爰於第五款明定事故機關得視個案情形，採取其他得即時有效防止個資事故擴大之應變措施。</p> <p>二、考量導致個資事故發生之原因多元，事故機關所得採取避免損害擴大之手段不應僵化，宜視個案情形彈性調整，爰於第二項明定事故機關</p>

<p>響人數、個人資料類別及筆數、潛在風險等因素擇定之。</p>	<p>辦理應變措施時，得綜合考量與事故有關之因素予以擇定。</p>
<p>第五條 受事故機關委託蒐集、處理及利用個人資料者，於本法適用範圍內知悉個資事故，視為委託機關知悉。</p> <p>前項情形，受託者應於知悉個資事故時，立即通知事故機關並保存通知紀錄。</p>	<p>一、依本法第四條規定，受委託蒐集、處理及利用個人資料者，於本法適用範圍內，視同委託機關。同法施行細則第七條及第八條亦規範，受託者依委託機關適用之規定及委託機關對其負有監督義務。是以，受託者於本法適用範圍內知悉個資事故，視為委託機關知悉。</p> <p>二、為使事故機關委託他人處理資料時之通報責任明確，參考歐盟一般資料保護規則（General Data Protection Regulation）第三十三條第二項規定，於第一項明定事故機關應於本法適用範圍內要求受託者應於知悉個資事故時，立即通知事故機關，同時明定受託者應保存通知紀錄，理屬當然。惟受託者違反第二項所定通知事故機關之義務，本法並無法對受託者裁罰；此時，事故機關除有行政罰法所定不予處罰之規定外（例如無故意或過失），以事故機關違反通知或通報義務之行為論處。至於受託者疏未通知，致事故機關遭行政裁罰，雙方關係應回歸委託契約或民法規定處理，併予敘明。</p>
<p>第六條 事故機關知悉個資事故後，應依本法第十二條第三項規定，以書面或電子方式製作相關紀錄，該紀錄應包括下列事項：</p>	<p>一、事故機關於知悉個資事故後，應妥為記錄對於個資事故之處理情形，以證明其於事故發生後善盡採行適當安全措施之義務，爰於本條明定</p>

<p>一、個資事故發生時間、地點及事故機關知悉個資事故時間、來源。</p> <p>二、個資事故發生原因、所涉受影響當事人人數及個人資料類別、筆數。</p> <p>三、依第二條規定通知當事人之情形。</p> <p>四、依第三條規定通報之情形。</p> <p>五、已採取即時有效防止損害擴大之應變措施及後續因應措施。</p> <p>六、個資事故所生之影響。</p> <p>七、調查方式、過程、結果及相關佐證資料。</p> <p>八、倘有違反本辦法所定情事，經主管機關令限期改正，就改正措施之處置歷程及相關佐證資料。</p> <p>前項相關紀錄，應於知悉個資事故之翌日起至少保存五年。但其他法規有較長之規定者，依其規定。</p>	<p>事故機關應製作相關紀錄及其應載事項。</p> <p>二、鑑於個資事故通知當事人及通報主管機關之義務，均以知悉個資事故起算，爰明定個資事故相關紀錄應自該知悉個資事故之翌日起至少保存五年。</p>
<p>第七條 本辦法施行日期，由主管機關定之。</p>	<p>配合本法修正期程，明定施行日期由主管機關定之。</p>

檔 號：
保存年限：

交通部 函

地址：100299臺北市仁愛路1段50號
傳真：(02)2382-0655
聯絡人：施先生
電話：(02)2349-2838

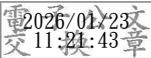
受文者：交通部民用航空局

發文日期：中華民國115年1月23日
發文字號：交科字第1150002621號
速別：普通件
密等及解密條件或保密期限：
附件：如文(1150002621-0-0.PDF、1150002621-0-1.pdf)

主旨：函轉個人資料保護委員會籌備處檢送115年1月22日個資籌
科字第1150600008號公告影本1份，請查照。

說明：依據個人資料保護委員會籌備處115年1月22日個資籌科字
第1150600008B號函辦理。

正本：部內各單位、部屬各機關(構)

副本：

裝

訂

線

檔 號：

保存年限：

個人資料保護委員會籌備處 函

地址：100011臺北市中正區館前路77號5樓

承辦人：蘇柏菁

電話：(02)3356-8016分機243

傳真：(02)3356-8012

電子信箱：pcsu@pdpc.gov.tw

受文者：交通部

發文日期：中華民國115年1月22日

發文字號：個資籌科字第1150600008B號

速別：普通件

密等及解密條件或保密期限：

附件：如主旨(115年1月22日個資籌科字第1150600008號公告影本1份.pdf)

主旨：檢送本籌備處115年1月22日個資籌科字第1150600008號公告影本1份。

正本：總統府、國家安全會議、行政院、立法院、司法院、考試院、監察院、內政部、外交部、國防部、財政部、教育部、法務部、經濟部、交通部、勞動部、衛生福利部、農業部、文化部、環境部、數位發展部、國家科學及技術委員會、國家發展委員會、大陸委員會、金融監督管理委員會、海洋委員會、僑務委員會、國軍退除役官兵輔導委員會、原住民族委員會、客家委員會、行政院公共工程委員會、行政院主計總處、行政院人事行政總處、中央銀行、國立故宮博物院、中央選舉委員會、公平交易委員會、國家通訊傳播委員會、運動部、國家運輸安全調查委員會、不當黨產處理委員會、核能安全委員會、各直轄市政府、各直轄市議會、各縣市政府、各縣市議會

副本：



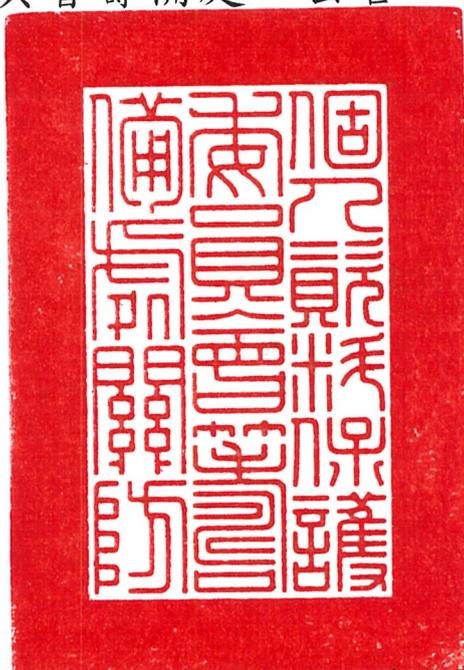
裝

訂

線

個人資料保護委員會籌備處 公告

發文日期：中華民國115年1月22日
發文字號：個資籌科字第1150600008號
附件：如公告事項三



主旨：預告訂定「個人資料檔案安全維護管理辦法」草案。

依據：行政程序法第一百五十四條第一項。

公告事項：

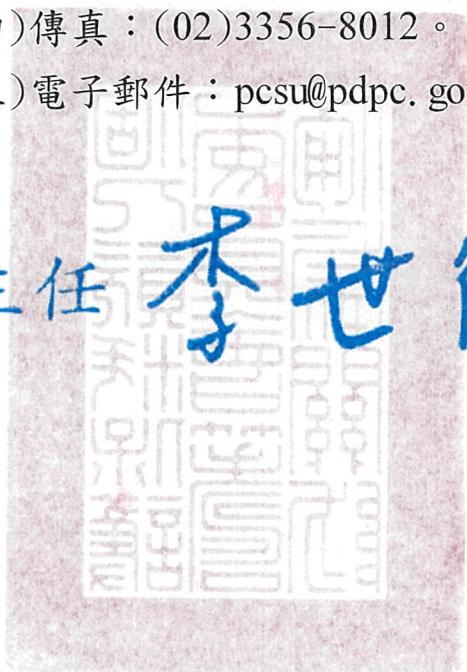
- 一、訂定機關：個人資料保護委員會（俟該會成立後訂定發布）。
- 二、訂定依據：個人資料保護法第十八條第二項及第二十條之一第二項。
- 三、「個人資料檔案安全維護管理辦法」草案如附件。本案另登載於本籌備處網站（網址：<https://www.pdpc.gov.tw/>）「最新消息」項下網頁、本籌備處「主管法規查詢系統」網站（網址：<https://law.pdpc.gov.tw/>）「草案預告」項下網頁及「公共政策網路參與平台」網站之「眾開講」（網址：<https://join.gov.tw/policies/>）。
- 四、對於本公告內容有任何意見或修正建議者，請於本公告刊登公報次日起60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）電話：(02)3356-8016分機243、232。



(四) 傳真：(02)3356-8012。

(五) 電子郵件：pcsu@pdpc.gov.tw。

主任 李世德



裝

訂



線

個人資料檔案安全維護管理辦法草案總說明

因應個人資料保護委員會成立，為落實資訊隱私權保障，兼顧個人資料檔案安全維護並促進合理利用，依據個人資料保護法(以下簡稱本法)第十八條第二項、第二十條之一第二項授權，就個人資料檔案安全維護事項、管理機制、應採取之措施及其他相關事項之辦法，由主管機關定之。

建立並實施個人資料檔案管理機制及安全維護措施為保障個人資料安全必要作為，為促進相關規範事項具有一致性，並確保對於個人資料之保護與管理，均能達到一定水準，爰訂定共通性規範，提供公務機關或非公務機關據以制定內部管理制度及安全維護控制措施，作為實施個人資料保護相關作業之基本準則，亦作為個人資料檔案安全維護最低限度之要求。

參考本法與施行細則、各機關所定個人資料檔案安全維護辦法、國際隱私保護法規、原則要項及個人資料管理趨勢，機關應衡酌持有之個人資料檔案類別、數量、機關特性、業務需求等，配置合理資源，實施個人資料安全維護作為；為協助公務機關或非公務機關針對個人資料檔案採取適當之安全維護措施，並持續精進及優化個人資料檔案安全維護事項，透由制定及落實組織上與程序上必要之管理，降低個人資料蒐集、處理及利用活動之安全風險，爰擬具「個人資料檔案安全維護管理辦法」(以下簡稱本辦法)草案，其要點如下：

一、本辦法訂定依據、目的、名詞定義與個人資料檔案筆數計算方式及增減適用。(草案第一條至第四條)

二、界定個人資料之管理範圍。(草案第五條)

三、建立事故之預防、通報及應變機制。(草案第六條)

四、對蒐集、處理及利用個人資料業務流程之人員採取安全管理措施。(草案第七條)

五、定期實施個人資料保護認知宣導及教育訓練。(草案第八條)

六、對保有電子個人資料檔案之設備採取安全管理措施。(草案第九條)

七、採取適當之實體安全措施以保護存放個人資料之場域。(草案第十條)

八、特種個人資料檔案安全管理。(草案第十一條)

- 九、機關自行或委外設置、開發之資通系統存取安全控制措施。（草案第十二條）
- 十、機關自行或委外設置、開發之資通系統事件日誌記錄及保存。（草案第十三條）
- 十一、機關自行或委外設置、開發之資通系統儲存之個人資料定期備份及保護措施。（草案第十四條）
- 十二、個人資料刪除及業務終止後個人資料處理方法。（草案第十五條）
- 十三、訂定個人資料檔案安全維護計畫。（草案第十六條）
- 十四、配置個人資料保護管理人員。（草案第十七條）
- 十五、定期清查作業流程與個人資料現況並文件化。（草案第十八條）
- 十六、個人資料之風險評估及管理機制。（草案第十九條）
- 十七、事故之通知、通報及應變機制之演練。（草案第二十條）
- 十八、定期實施管理制度及差異化教育訓練。（草案第二十一條）
- 十九、個人資料檔案安全管理。（草案第二十二條）
- 二十、機關維運自行或委外設置、開發之資通系統之資訊安全措施。（草案第二十三條）
- 二十一、內部個人資料安全稽核及受託者稽核。（草案第二十四條）
- 二十二、個人資料使用紀錄及證據保存。（草案第二十五條）
- 二十三、個人資料安全維護之整體持續改善機制。（草案第二十六條）
- 二十四、非公務機關於過渡期間個人資料檔案安全維護管理辦法適用情形。（草案第二十七條）
- 二十五、本辦法之施行日期。（草案第二十八條）

個人資料檔案安全維護管理辦法草案

條文	說明
第一章 總則	章名。
第一條 本辦法依個人資料保護法（以下簡稱本法）第十八條第二項及第二十條之一第二項規定訂定之。	明定本辦法訂定之依據。
第二條 公務機關或非公務機關應按其機關規模、特性與其保有之個人資料檔案，衡酌資源之合理分配，規劃、訂定、檢討及修正內部管理機制，落實安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。	本辦法適用於公務機關或非公務機關，其所具資源、規模與保有之個人資料檔案相異。機關應審酌其組織規模、業務屬性、經營模式、保有之個人資料檔案類型或數量等具體情狀，基於比例原則採取適當管理機制及安全維護措施並落實之。
<p>第三條 本辦法用詞，定義如下：</p> <p>一、大型非公務機關：指依法辦理公司、有限合夥或商業登記，而非屬中小企業認定標準第二條所稱中小企業，且保有當事人個人資料檔案筆數達一萬筆以上之非公務機關。</p> <p>二、風險評估：包括風險識別、風險分析及風險評量之過程。</p> <p>三、資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。</p>	<p>一、參考經濟部「中小企業認定標準」第二條所定之標準，排除中小企業，明定具有一定經濟規模之大型企業保有大量個人資料檔案者為大型非公務機關，其執行法令遵循之資源及能力相對充足，採行加強管理機制，為第一款規定。</p> <p>二、參考行政院及所屬各機關風險管理及危機處理作業原則及行政院及所屬各機關風險管理及危機處理作業手冊之規範，為第二款規定。</p> <p>三、參照資通安全管理法第三條第一款之定義，為第三款規定。</p>
<p>第四條 非公務機關保有個人資料檔案筆數，以非公務機關單日所保有每一自然人之每一蒐集特定目的加總計算。</p> <p>非公務機關保有個人資料檔案筆數未達一萬筆，於本辦法施行後，因直接或間接蒐集而達一萬筆者，應於保有筆數達一萬筆之日起算六個月內採行本辦法所定大型非公務機關安全維護事項及管理機制。</p> <p>大型非公務機關因刪除、銷毀或其他方法致保有個人資料檔案筆數減少，且連續二年期間保有個人資料檔案筆數未達一萬筆之業者，得不適用第十六條至第二十六條之規定。但嗣後因直接或間接蒐集而致保有個人資料檔案筆數達一萬筆以上者，應於保有筆數達一萬筆之日起算六個月內，恢復適用本條規定。</p>	<p>一、本條第一項非公務機關保有個人資料檔案筆數之計算方式，所稱「單日」係指機關盤點當日，筆數依個人資料蒐集之不同目的而個別累加計算。舉例同一自然人之個人資料檔案蒐集為「網站會員資料」及「內部員工資料」之蒐集特定目的不同，則加總其個人資料檔案筆數。</p> <p>二、非公務機關因組織或業務規模擴大等因素，致個人資料檔案筆數增加，應重新盤點個人資料檔案筆數，並應於保有筆數達一萬筆之日起算六個月內一併採行本辦法所定大型非公務機關安全維護事項及管理機制。</p> <p>三、考量大型非公務機關依法令主動或依當事人之請求刪除個人資料、或可能因為業務規模或經營之改變等因素，致保有個人資料檔案筆數有所增</p>

	減，爰於第二項及第三項明定非公務機關適用、不再適用及重新適用本辦法對於大型非公務機關之相關規範。
第二章 公務機關或非公務機關共通安全維護措施	一、章名。 二、本章明定公務機關或非公務機關必須採行之共通安全維護措施規定。
第五條 公務機關或非公務機關應依個人資料保護相關法令，定期清查確認所保有之個人資料現況，界定個人資料管理範圍。	個人資料之蒐集、處理或利用係屬連續且變動之過程，透過定期盤點與現況清查，可釐清保有之個人資料之種類、數量及法律依據等，並據此確認資料之正確性與保存必要性。爰明定公務機關或非公務機關應建立定期清查確認機制，以界定並調整應納入管理之範圍，避免因範圍界定不明或管理疏漏致生事故風險，並落實個人資料保護相關法令規範。
第六條 公務機關或非公務機關應依個人資料事故通知通報及應變辦法規定，建立個人資料事故之通報、通知及應變機制。	一、公務機關或非公務機關發生個人資料事故，應採行通知、通報及應變措施，並負保存事故紀錄之義務。 二、為確保公務機關或非公務機關運作事故之處置，應建立通知、通報、應變及檢討改善之機制。
第七條 公務機關或非公務機關應對蒐集、處理或利用個人資料業務流程之人員，採取下列人員安全管理措施，並定期檢視措施之適當性及必要性： 一、識別業務內容涉及個人資料蒐集、處理或利用之人員。 二、依組織業務特性、內容與需求，建立人員之保密義務、身分識別與鑑別及權限管控措施。 三、機關業務或職務異動時，異動人員於載有個人資料媒介物之交接、返還或資料刪除措施。	一、為使公務機關或非公務機關建立人員管理之體系，應識別業務涉及個人資料蒐集、處理或利用之人員，以達到權責分明，並有效追蹤及管理，為第一款規定。 二、公務機關或非公務機關辦理個人資料之蒐集、處理或利用，所屬人員直接或間接有取得個人資料可能性，應與其約定個人資料保密義務，以降低未經授權的人員濫用個人資料之風險。針對接觸個人資料之人員建立身分驗證機制，確保已識別為合法授權人員，並經鑑別其身分真確性方可存取個人資料，應依循最小權限原則配發必要權限，為第二款規定。 三、為避免人員業務異動或離職仍繼續保有機關內部個人資料致生風險，並確保機關對個人資料之控制，應落實存有個人資料之載體返還以及資料之刪除，為第三款規定。
第八條 公務機關或非公務機關應對所屬人員，定期施以個人資料保護認知宣導及教育訓練。	公務機關或非公務機關應教育所屬人員其所負之法律責任，確保其瞭解內部管理程序與要求，並因應內、外部環境變化之

	可能性，應定期辦理個人資料保護認知宣導及教育訓練。
<p>第九條 公務機關或非公務機關保有電子個人資料檔案，應採取下列設備安全管理措施：</p> <ol style="list-style-type: none"> 一、妥善保管並實施適宜之存取管制。 二、資通訊軟、硬體應適時進行必要更新或升級，並修補漏洞。 三、電腦應安裝防毒軟體或採用其他防護設備；防毒軟體應設定自動更新至最新版本病毒碼，且應啟動即時病毒防範機制，定期執行完整掃描作業，並針對惡意程式執行刪除。 	<p>公務機關或非公務機關使用資通訊軟、硬體，進行個人資料之蒐集、處理或利用，應妥善保管資訊資產與實施存取管制，並執行必要之資通訊軟、硬體升級更新與漏洞修補，建置與啟動即時病毒防範及惡意程式處理機制。</p>
<p>第十條 公務機關或非公務機關應採取適當之實體安全措施以保護存放個人資料之場域，其安全措施包括但不限於下列項目：</p> <ol style="list-style-type: none"> 一、場域進出：建立對於資訊機房及檔案庫房等管制區域之人員進出管理，僅允許經授權之人員進入。 二、監控系統：於資訊機房與檔案庫房等管制區域安裝監控系統，監控並記錄人員及個人資料之進出。 三、實體障礙：使用安全鎖、門禁系統等實體安全措施。 	<p>個人資料檔案為紙本或電子檔案形式，均須確保儲存媒介物之實體場域安全防護，實施如管制場域進出、設置監控系統及建立實體障礙等，以防止個人資料遭不當存取，並應考量風災、水災等環境威脅之防範措施，以降低發生個人資料事故之風險。</p>
<p>第十一條 公務機關或非公務機關保有本法第六條第一項有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料者，應針對載有前述個人資料之紙本或電子檔案採取下列資料安全管理措施：</p> <ol style="list-style-type: none"> 一、訂定紙本及使用可攜式設備或儲存媒體之管制規範。 二、保有個人資料檔案之媒介物於銷毀、報廢或轉作其他用途時，應採取適當防範措施。 三、處理過程有備份個人資料之需要時，應比照原件，依本辦法規定予以保護。 四、檔案安全加密措施。 五、資料安全傳輸措施。 六、安全銷毀機制。 	<ol style="list-style-type: none"> 一、特種個人資料如發生竊取、竄改、毀損、滅失或洩漏之事故其對當事人權益影響將更為嚴重，爰本條明定資料安全管理措施。 二、公務機關或非公務機關保有特種個人資料，應確保資料生命週期之安全，檔案資料儲存之媒介物之管制與安全防範措施。 三、依本法施行細則第五條之意旨，檔案備份資料應比照原件予以保護，另檔案資料儲存應加密及採取安全傳輸措施，並應於個人資料蒐集之特定目的消失或期限屆滿須刪除時，確保資料已安全銷毀且不可回復。

<p>第十二條 公務機關或非公務機關維運自行或委外設置、開發之資通系統蒐集、處理或利用個人資料，其帳號管理及存取安全控制措施應規範之範圍包括但不限於下列項目：</p> <ol style="list-style-type: none"> 一、使用者存取應採最小權限原則。 二、帳號安全管理及定期清查。 三、設置密碼並符合複雜性需求。 	<ol style="list-style-type: none"> 一、公務機關或非公務機關維運自行或委外設置、開發之資通系統蒐集、處理或利用個人資料者，明定資通系統存取控制至少應採取之安全控制措施，以降低資料遭未經授權存取並濫用之風險。 二、使用者存取個人資料應僅限於其執行業務所需最低限度之最小權限原則、建立完善之帳號生命週期管理機制，包含帳號之申請、審核、啟用、停用及註銷等流程。 三、應定期對現有帳號進行清查，以有效識別並移除不再使用或異常之帳號、以及強制使用者設置符合一定複雜性要求之密碼，並定期更換。
<p>第十三條 公務機關或非公務機關維運自行或委外設置、開發之資通系統蒐集、處理或利用個人資料，應執行下列事項：</p> <ol style="list-style-type: none"> 一、訂定日誌之記錄時間週期及留存政策，並保存適當期間。 二、確保資通系統具備記錄特定事件之功能，並決定應記錄之特定資通系統事件。 三、應記錄資通系統管理者帳號所執行之各項功能。 	<ol style="list-style-type: none"> 一、公務機關或非公務機關如有維運自行或委外設置、開發之資通系統蒐集、處理或利用個人資料者，為確保可有效進行個人資料事故之追查與鑑識，明定資通系統事件日誌與可歸責性至少應採取之安全控制措施。 二、機關應明確訂定資通系統日誌的記錄時間、週期及留存政策，確保資通系統具備記錄特定重要事件的功能。 三、機關應明定應記錄的特定資通系統事件（如使用者登入、登出、權限變更、資料存取、修改或刪除等敏感操作行為）、以及記錄並監控系統特權帳號所執行的各項操作。
<p>第十四條 公務機關或非公務機關維運自行或委外設置、開發之資通系統蒐集、處理或利用個人資料，應就資通系統儲存之個人資料定期備份，並應對備份資料採取適當之保護措施及確保其可用性。</p>	<p>公務機關或非公務機關維運自行或委外設置、開發之資通系統蒐集、處理及利用個人資料者，明定資通系統營運持續計畫應就儲存之個人資料定期備份、對備份檔案採取等同原件之保護，並確保實施備份資料取代或回復後之檔案可用性。</p>
<p>第十五條 公務機關或非公務機關依本法第十一條第三項規定刪除個人資料，應採取適當刪除措施使資料不可回復，並留存刪除紀錄。</p> <p>前項機關於職務或業務終止後，其所蒐集、處理或利用之個人資料應依下列方式處理，並留存下列紀錄：</p> <ol style="list-style-type: none"> 一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。 	<ol style="list-style-type: none"> 一、公務機關或非公務機關應確保個人資料之銷毀程序，使其無法還原或重建，並留存可供查核之紀錄。 二、機關於職務或業務終止後其所蒐集、處理及利用之個人資料，應採取銷毀、移轉或其他刪除、停止處理或利用之方法，均應予記錄。 三、所有刪除與職務或業務終止後處理的紀錄，均應留存至少五年，以供於

<p>二、移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得蒐集該個人資料之合法依據。</p> <p>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。</p> <p>前二項紀錄應留存至少五年。</p>	<p>當事人權利主張時進行追溯或供主管或上級機關進行監督查核。</p>
<p>第三章 公務機關或大型非公務機關強化安全維護措施</p>	<p>一、章名。</p> <p>二、本章明定公務機關或大型非公務機關必須採行之強化安全維護措施規定。非公務機關依其個人資料保護需要及目的性，亦可採行本章措施。</p>
<p>第十六條 為實施第二條內部管理機制，公務機關或大型非公務機關應訂定個人資料檔案安全維護計畫(以下簡稱本計畫)，包括但不限於下列項目：</p> <p>一、配置管理之人員及相當資源。</p> <p>二、界定個人資料之範圍。</p> <p>三、個人資料之風險評估及管理機制。</p> <p>四、事故之預防、通報及應變機制。</p> <p>五、人員管理、認知宣導及教育訓練。</p> <p>六、設備及場域安全管理。</p> <p>七、資料安全、資訊安全。</p> <p>八、資料安全稽核機制。</p> <p>九、使用紀錄、軌跡資料及證據保存。</p> <p>十、個人資料安全維護之整體持續改善。</p> <p>前項計畫之訂定或修正，應經公務機關個人資料保護長、非公務機關代表人、管理人、其他代表人或其指派之適當人員核定。</p>	<p>一、公務機關或大型非公務機關應制定個人資料檔案安全維護計畫，以系統性與文件化作法達成個人資料檔案管理目的，具體建構內部管理機制及安全維護事項等規劃俾據以實施。</p> <p>二、個人資料檔案安全維護計畫內容應包含本辦法第五條至第二十六條規定之具體實踐內容。</p> <p>三、為強化組織治理及領導階層責任，個人資料檔案安全維護計畫之訂定或修正，應由機關之個人資料保護最高管理者或其指派之適當人員審查、確認及核定。</p>
<p>第十七條 大型非公務機關應指定個人資料保護管理專責人員，並設置個人資料保護管理執行小組與查核人員，以辦理本辦法所定安全維護事項及管理機制之經常性工作。</p> <p>大型非公務機關應確保管理專責人員及查核人員具備適當專業能力，且兩者不得兼任。</p>	<p>一、本條為本辦法第七條之強化規定。</p> <p>二、大型非公務機關應指定專責人員辦理個人資料檔案安全維護事項，以防止個人資料事故，並應設置個人資料保護管理執行小組，任務包括機關內個人資料保護政策研議、執行、稽核、改善等事項，並應訂定成員組成及小組運作相關事項，為第一項規定。</p> <p>三、辦理個人資料安全稽核，為確保稽核之獨立性，應要求查核人員與執行個人資料管理之管理人員不得互相兼任；並為強化人員專業性，應規範管理人員、查核人員具備適當專業能</p>

<p>第十八條 公務機關或大型非公務機關於界定個人資料管理範圍時，應定期清查其個人資料蒐集、處理或利用之流程，與其所保有之個人資料現況，並建立個人資料檔案盤點清冊及個人資料蒐集、處理或利用流程之說明文件。</p> <p>前項盤點清冊應包括但不限於下列項目：</p> <ol style="list-style-type: none"> 一、保有單位。 二、個人資料之項目、類別、型態、數量。 三、蒐集之特定目的、方式、來源。 四、依本法第八條或第九條向當事人告知之方式，或得免為告知之情形。 五、蒐集、處理及利用相關業務或程序。 六、依本法第六條第一項、第十六條或第二十條第一項為目的外利用之情形。 七、保存方式、期限及銷毀方式。 	<p>力，為第二項規定。</p> <ol style="list-style-type: none"> 一、本條為本辦法第五條之強化規定。 二、公務機關或大型非公務機關應每年清查盤點個人資料蒐集、處理及利用所涉之業務流程，及所保有個人資料之現況，以界定個人資料檔案之管理範圍，並建立個人資料盤點清冊及流程說明文件等文件化資訊，為第一項規定。 三、公務機關或大型非公務機關應建立個人資料檔案盤點清冊，並明定盤點清冊至少應包含項目，為第二項及各款規定。
<p>第十九條 公務機關或大型非公務機關，應依據前條所界定之個人資料管理範圍，針對其保有之個人資料現況與其業務涉及個人資料蒐集、處理或利用之流程，每年定期識別、分析及評估可能面臨之風險，並根據風險評估結果，採行適當安全維護措施。</p> <p>前項風險評估應包括但不限於下列事項：</p> <ol style="list-style-type: none"> 一、個人資料之項目、類別、型態、數量。 二、處理個人資料之方法、技術。 三、內部及外部之潛在威脅。 	<ol style="list-style-type: none"> 一、公務機關或大型非公務機關完成個人資料檔案盤點及管理範圍界定，於製作個人資料檔案盤點清冊後，應每年定期識別、分析及評估可能面臨之風險。 二、依風險評估結果列出可行的風險處理對策，評估接受、規避、抑減或移轉風險，採取對應適當安全維護管理機制及措施，並擬定及實施風險處理計畫。
<p>第二十條 公務機關或大型非公務機關應依據前條風險評估結果，定期辦理個人資料事故之通報、通知及應變機制演練，以確保機制運行之有效性。</p>	<ol style="list-style-type: none"> 一、本條為本辦法第六條之強化規定。 二、公務機關或大型非公務機關應落實個人資料事故應變處理流程，提升回應效能、強化面對個人資料事故之韌性，機關應依據風險評估結果，每年定期辦理個人資料事故通知、通報與應變機制演練。

<p>第二十一條 公務機關或大型非公務機關應根據職務或業務規模、個人資料檔案保有量、業務性質等差異，定期辦理必要之教育訓練，確保本法第十八條第二項指定之專人或第十七條第一項指定之專責人員明瞭內部與外部規定之要求、責任範圍與個人資料保護機制、程序及措施。</p>	<p>一、本條為本辦法第八條之強化規定。 二、公務機關或大型非公務機關應評估有關條件，明定妥適頻率定期辦理管理制度及差異化(如通識及專業課程)之個人資料保護教育訓練，確保個人資料檔案保護專人或專責人員具備工作對應之責任、意識及能力。 三、訓練內容包含內、外部相關法令遵循權責任務及相關規範、機制、程序及措施之要求，並應進行訓練成效評估，俾利正確實施個人資料檔案安全維護事項，長期並建立機關個人資料保護文化。</p>
<p>第二十二條 公務機關或大型非公務機關保有紙本或電子個人資料檔案，應採取下列資料安全管理措施：</p> <ol style="list-style-type: none"> 一、訂定紙本及使用可攜式設備或儲存媒體之管制規範。 二、保有個人資料檔案之媒介物於銷毀、報廢或轉作其他用途時，應採取適當防範措施。 三、處理過程具備份個人資料之需要時，應比照原件，依本辦法規定予以保護之。 <p>保有個人資料檔案屬於本法第六條以外之個人資料，經第十九條風險評估結果，屬優先處理項目且為執行業務所必要者，得採取第十一條第四款、第五款及第六款之安全管理措施。</p>	<p>一、公務機關或大型非公務機關應落實個人資料保護之課責性、公平性及可執行性，評估機關規模、資源及保有一定數量個人資料檔案之影響。 二、第一項明定機關就所保有之本法第六條以外之個人資料，採行本辦法第十一條第一款至第三款之資料安全管理措施；惟個人資料檔案如經本辦法第十九條風險評估結果，認有必要優先處理安全風險且為執行業務所必要者，得評估併採取本辦法第十一條第四款至第六款之資料安全管理措施。</p>
<p>第二十三條 公務機關或大型非公務機關，維運自行或委外設置、開發之資通系統蒐集、處理或利用個人資料，應採取下列資訊安全措施：</p> <ol style="list-style-type: none"> 一、使用者帳號管理、身分鑑別及保護機制。 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、個人資料檔案與資料庫之存取控制及保護監控措施。 五、防止外部網路入侵對策。 六、非法或異常使用行為之監控及因應機制。 七、訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。 	<p>一、本條為本辦法第十二條、第十三條及第十四條之強化規定。 二、公務機關或大型非公務機關維運自行或委外設置、開發之資通系統蒐集、處理或利用個人資料，應採行資訊安全措施，以防止個人資料事故發生。 三、提供對外服務之資通系統潛在風險高，個人資料外洩之影響層面鉅大，系統上線前應辦理源碼檢測、弱點掃描及滲透測試，並完成弱點、漏洞修補作業；另考量資通訊科技發展日新月異，資訊安全亦與時俱進，爰系統上線後仍應持續辦理前述安全性掃描檢測及弱點、漏洞修補作業。</p>

<p>八、儲存之個人資料定期備份。</p> <p>九、資通系統如提供對外服務，系統上線前應辦理源碼檢測、弱點掃描及滲透測試，並完成弱點、漏洞修補作業；系統上線後應持續辦理。</p> <p>前項各款所定措施，應定期評估其有效性及檢討改善。</p>	<p>四、第二項明定機關應定期演練前項各款所定措施，以熟悉整體作業流程，及時發現問題並檢討改善，俾周全資訊安全防護作業。</p>
<p>第二十四條 公務機關或大型非公務機關應訂定內部個人資料安全稽核機制，每年應至少辦理一次稽核機關實施個人資料安全維護事項與管理機制之情形及成效。</p> <p>前項內部稽核機制應包括但不限於下列項目：</p> <ol style="list-style-type: none"> 一、稽核項目及內容。 二、執行稽核之合理頻率。 三、稽核結果之紀錄。 <p>公務機關或大型非公務機關具委外辦理蒐集、處理或利用個人資料之情形者，委託機關與受託機關應於委託契約或相關文件中，明確約定其內容，並每年至少辦理一次稽核受託者執行情形及記錄稽核結果備查。</p> <p>第一項及第三項稽核結果應向公務機關首長、非公務機關代表人、管理人或其他有代表權人報告，並落實改善；稽核結果之紀錄應保存五年。</p>	<ol style="list-style-type: none"> 一、為確認安全維護管理機制及措施之落實情形及有效性，並強化機關內、外部相關控制機制，明定公務機關或大型非公務機關應由查核人員每年定期辦理內部稽核；若稽核發現缺失，應立即進行改善，為第一項規定。 二、明定內部稽核機制至少應包含之項目，為第二項規定。 三、委託他人蒐集、處理或利用個人資料之行為，將使個人資料置於可控制範圍以外之區域，委託方應善盡對受託者之監督管理責任，有必要與受託方就委託管理為妥善約定。公務機關或大型非公務機關應就前述約定內容，每年定期對受託者進行稽核作業，為第三項規定。 四、公務機關或大型非公務機關內部稽核或對受託者稽核之結果應向機關首長或代表人等報告並落實改善，並明定每次稽核結果紀錄應至少保存五年，以對應提供法令遵循及相關規範等之內、外部查核，為第四項規定。
<p>第二十五條 公務機關或大型非公務機關執行本計畫所定各種個人資料保護機制、程序及措施，應保存下列紀錄：</p> <ol style="list-style-type: none"> 一、個人資料之蒐集、處理或利用紀錄。 二、落實安全維護措施之證據。 三、當事人權利行使之紀錄。 <p>前項紀錄之保存期間，除本辦法另有規定者外，應留存至少五年。</p>	<ol style="list-style-type: none"> 一、公務機關或大型非公務機關應佐證個人資料檔案安全保護制度之落實，並為保護當事人權利及避免訴訟爭議，明定機關應就個人資料之流向及處理過程之完整紀錄、安全維護措施之執行紀錄、當事人權利行使紀錄等妥為保存。 二、相關紀錄之保存期限，參考對應本法第三十條規定，明定業者應保存至少五年。
<p>第二十六條 公務機關或大型非公務機關應訂定包含下列措施之整體持續改善機制：</p> <ol style="list-style-type: none"> 一、安全維護計畫未落實執行時之矯正預防措施。 	<p>公務機關或大型非公務機關應持續改善、有效執行個人資料檔案之安全保護事項，明定應追蹤並持續關注計畫未落實執行之矯正預防措施，並配合法令訂定或修正及參酌內、外部因素，定期檢討所定之計畫</p>

<p>二、應配合法令訂定或修正，參酌執行業務狀況、技術發展等因素，定期檢視所定之規定、計畫合宜性，必要時應予修正。</p>	<p>是否合宜，並進行必要修正，俾利個人資料檔案安全維護事項得持續滾動檢討改善。</p>
<p>第四章 附則</p>	<p>章名。</p>
<p>第二十七條 本法第五十一條之一第一項及第二項公告範圍內之非公務機關，應適用中央目的事業主管機關依同條第四項授權訂定之辦法。但中央目的事業主管機關未訂定相關辦法，或本辦法規定較為嚴格者，適用本辦法之規定。</p>	<p>本法第五十一條之一訂有六年過渡期規定，部分非公務機關於過渡期間仍由中央目的事業主管機關或直轄市、縣（市）政府管轄，為使前述非公務機關明確理解本辦法與其他中央目的事業主管機關所定辦法間之適用關係，為本條規定。</p>
<p>第二十八條 本辦法施行日期，由主管機關定之。</p>	<p>配合本法修正期程，明定施行日期由主管機關定之。</p>

交通部 函

地址：100299臺北市仁愛路1段50號
傳真：(02)2382-0655
聯絡人：施先生
電話：(02)2349-2838

受文者：交通部民用航空局

發文日期：中華民國115年1月23日
發文字號：交科字第1150002623號
速別：普通件
密等及解密條件或保密期限：
附件：如文(1150002623-0-0. pdf、1150002623-0-1. pdf、1150002623-0-2. pdf、1150002623-0-3. PDF)

主旨：函轉個人資料保護委員會籌備處檢送「個人資料保護法施行細則」部分條文修正草案預告公告，並附「個人資料保護法施行細則」部分條文修正草案總說明及條文對照表各1份，請查照。

說明：

- 一、依據個人資料保護委員會籌備處115年1月22日個資籌法字第1140400391B號函辦理。
- 二、旨揭草案同時登載於該籌備處全球資訊網站/最新消息(網址：<https://www.pdpc.gov.tw/News/20/>)、該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台/眾開講/法令草案預告(網站：<https://join.gov.tw/policies/>)
- 三、對於本公告內容有任何相關意見或修正建議，請於預告期間內向該籌備處或於說明二之平台提出。另請協助轉知所屬機關、學校及所管行業之公(協)會，俾廣納各界意見。

正本：部內各單位、部屬各機關(構)

副本：

個人資料保護委員會籌備處 函

地址：100011臺北市中正區館前路77號5樓
承辦人：林威廷
電話：(02)3356-8016
傳真：(02)3356-8012
電子信箱：w3272001@pdpc.gov.tw



受文者：交通部

發文日期：中華民國115年1月22日
發文字號：個資籌法字第1140400391B號
速別：普通件
密等及解密條件或保密期限：
附件：如主旨(個人資料保護法施行細則部分條文修正草案總說明.pdf、個人資料保護法施行細則部分條文修正草案條文對照表.pdf、公告.pdf)

主旨：檢送「個人資料保護法施行細則」部分條文修正草案預告公告，並附「個人資料保護法施行細則」部分條文修正草案總說明及條文對照表各1份，請查照。



說明：

- 一、旨揭草案同時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台/眾開講/法令草案預告(網站：<https://join.gov.tw/policies/>)。
- 二、對於本公告內容有任何相關意見或修正建議，請於預告期間內向本籌備處或於說明二之平台提出。另請協助轉知所屬機關、學校及所管行業之公(協)會，俾廣納各界意見。

正本：總統府、國家安全會議、行政院、立法院、司法院、考試院、監察院、內政部、外交部、國防部、財政部、教育部、法務部、經濟部、交通部、勞動部、衛生福利部、農業部、文化部、環境部、數位發展部、國家科學及技術委員會、國家發展委員會、大陸委員會、金融監督管理委員會、海洋委員會、僑務委員會、國軍退除役官兵輔導委員會、原住民族委員會、客家委員會、行政院公共工程委員會、行政院主計總處、行政院人事行政總處、中央銀行、國立故宮博物院、中央選舉委員會、公平交易委員會、國家通訊傳播委員會、運動部、國家運輸安全調查

委員會、不當黨產處理委員會、核能安全委員會、各直轄市及各縣(市)政府、各直轄市及各縣(市)議會

副本： 



裝



訂

線

個人資料保護委員會籌備處 公告

發文日期：中華民國115年1月22日
發文字號：個資籌法字第1140400391號
附件：如公告事項三



主旨：預告修正「個人資料保護法施行細則」部分條文。

依據：行政程序法第一百五十一條第二項準用第一百五十四條第一項。

公告事項：

- 一、修正機關：個人資料保護委員會(俟該會成立後修正發布)。
- 二、修正依據：個人資料保護法第五十五條。
- 三、「個人資料保護法施行細則」部分條文修正草案如附件。本案另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台/眾開講/法令草案預告(網站：<https://join.gov.tw/policies/>)。
- 四、對本公告內容有任何意見或修正建議者，請於本公告刊登次日起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)電話：(02)3356-8016分機252、216

(四) 傳真：(02)3356-8012

(五) 電子郵件：w3272001@pdpc.gov.tw

主任 李世德



裝

訂

線

個人資料保護法施行細則部分條文修正草案總說明

原電腦處理個人資料保護法施行細則於八十五年五月一日訂定發布全文四十六條，嗣於一百零一年九月二十六日修正發布名稱為個人資料保護法施行細則（以下簡稱本細則）及全文三十三條；並自一百零一年十月一日施行。本細則最近一次修正公布日期為一百零五年三月二日；並自一百零五年三月十五日施行。

個人資料保護法（以下簡稱本法）部分條文修正草案已於一百十四年十月十七日經立法院三讀通過，並於同年十一月十一日經總統公布，為配合本法修正條文內容，及針對現行條文作必要之調整，以強化個人資料保護機制，爰擬具本細則部分條文修正草案，其修正要點如下：

- 一、配合本法修正條文第十二條、第十八條、第二十條之一等規定授權主管機關就事故發生後之通報（知）、個人資料檔案安全維護、個人資料保護長等人員之職掌、職能條件、訓練等事項訂定相關辦法，爰刪除相關規定。（修正條文第十二條、第二十二條、第二十四條及第二十五條）
- 二、本細則有關無從識別特定當事人之定義，參酌憲法法庭一百十一年憲判字第十三號判決意旨予以修正。（修正條文第十七條）
- 三、配合本法修正條文第二十一條之五規定，增訂情報機關之定義。（修正條文第二十九條）
- 四、配合本法修正條文第五十二條規定，修正公益團體之定義。（修正條文第三十一條）
- 五、過渡條款規定已無繼續適用之必要，爰予刪除。（修正條文第三十二條）
- 六、配合個人資料保護委員會之成立，修正本細則施行日期之指定機關。（修正條文第三十三條）

個人資料保護法施行細則部分條文修正草案條文對照表

修正條文	現行條文	說明
<p>第十二條 (刪除)</p>	<p>第十二條 <u>本法第六條第一項但書第二款及第五款所稱適當安全維護措施、第十八條所稱安全維護事項、第十九條第一項第二款及第二十七條第一項所稱適當之安全措施</u>，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。</p> <p style="padding-left: 2em;"><u>前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：</u></p> <p style="padding-left: 2em;">一、<u>配置管理之人員及相當資源。</u></p> <p style="padding-left: 2em;">二、<u>界定個人資料之範圍。</u></p> <p style="padding-left: 2em;">三、<u>個人資料之風險評估及管理機制。</u></p> <p style="padding-left: 2em;">四、<u>事故之預防、通報及應變機制。</u></p> <p style="padding-left: 2em;">五、<u>個人資料蒐集、處理及利用之內部管理程序。</u></p> <p style="padding-left: 2em;">六、<u>資料安全管理及人員管理。</u></p> <p style="padding-left: 2em;">七、<u>認知宣導及教育訓練。</u></p> <p style="padding-left: 2em;">八、<u>設備安全管理。</u></p> <p style="padding-left: 2em;">九、<u>資料安全稽核機制。</u></p>	<p>一、<u>本條刪除。</u></p> <p>二、本法修正條文第十八條第二項後段、第二十七條之一第二項規定，已授權由主管機關就公務機關與非公務機關之個人資料檔案安全維護、管理機制、應採取之措施及其他相關事項訂定辦法，爰配合刪除本條規定。</p>

	<p><u>十、使用紀錄、軌跡資料及證據保存。</u></p> <p><u>十一、個人資料安全維護之整體持續改善。</u></p>	
<p>第十七條 本法第六條第一項但書第四款、第九條第二項第四款、第十六條但書第五款、第十九條第一項第四款及第二十條第一項但書第五款所稱無從識別特定當事人，指<u>運用當時存在技術方法，使該個人資料依其呈現方式至少已無從直接識別特定自然人。</u></p>	<p>第十七條 本法第六條第一項但書第四款、第九條第二項第四款、第十六條但書第五款、第十九條第一項第四款及第二十條第一項但書第五款所稱無從識別特定當事人，指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者。</p>	<p>鑒於現行條文所稱個人資料「無從識別特定當事人」，是否指個人資料應處理至無從直接或間接識別特定個人，於實務上時生爭議，依憲法法庭一百十一年憲判字第十三號判決意旨，本法第六條第一項但書第四款等規定所稱「無從識別特定之當事人」，排除「可直接識別該個人」、「完全匿名且無還原可能性，因此不在個資法保護範圍內」之資料型態。準此，為使現行條文規範意旨更為明確，爰參照上開憲法法庭判決，明定本條所稱無從識別特定當事人，係指運用當時存在技術方法，使該個人資料依其呈現方式至少已無從直接識別特定自然人，但仍屬可能間接識別特定自然人之情形。</p>
<p>第二十二條 (刪除)</p>	<p>第二十二條 <u>本法第十二條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以</u></p>	<p>一、<u>本條刪除。</u></p> <p>二、本法修正條文第十二條第四項規定，授權由主管機關訂定通知當事人之內容、方式、時限等事項，俾利事故機關妥適履行其通知義務，本條已無規範之必要，爰予刪除。</p>

	<p><u>網際網路、新聞媒體或其他適當公開方式為之。</u></p> <p><u>依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。</u></p>	
第二十四條（刪除）	<p><u>第二十四條 公務機關保有個人資料檔案者，應訂定個人資料安全維護規定。</u></p>	<p>一、<u>本條刪除。</u></p> <p>二、本法修正條文第十八條增訂第二項後段規定，授權由主管機關訂定公務機關個人資料檔案安全維護事項、管理機制、應採取之措施及其他相關事項之辦法，本條已無規範之必要，爰予刪除。</p>
第二十五條（刪除）	<p><u>第二十五條 本法第十八條所稱專人，指具有管理及維護個人資料檔案之能力，且足以擔任機關之個人資料檔案安全維護經常性工作之人員。</u></p> <p><u>公務機關為使專人具有辦理安全維護事項之能力，應辦理或使專人接受相關專業之教育訓練。</u></p>	<p>一、<u>本條刪除。</u></p> <p>二、本法修正條文第十八條第四項已明定主管機關應妥為規劃推動個人資料保護長、專人等人員之職能培訓事宜，並於第五項規定授權由主管機關就該等人員之職掌、職能條件、訓練等事項訂定辦法，本條爰予刪除。</p>
第二十九條 <u>本法第二十一條之五所稱情報機關，指國家情報工作法第三條第一項第一款及第二項規定之機關。</u>	<p><u>第二十九條 依本法第二十二條規定實施檢查時，應注意保守秘密及被檢查者之名譽。</u></p>	<p>一、有關檢查人員實施檢查時應注意保密及被檢查者之名譽，於本法修正條文第二十二條第六項已明定，爰予刪除。</p> <p>二、配合本法第二十一條之五增訂情報機關豁免公務機關內、外部行</p>

		政機監督之規定，爰參考資通安全管理法施行細則第二條規定，於本條增訂情報機關之定義。
第三十一條 本法第五十二條第一項所稱公益團體，指依民法或其他法律設立並具備個人資料保護專業能力之公益社團法人及財團法人。	第三十一條 本法第五十二條第一項所稱之公益團體，指依民法或其他法律設立並具備個人資料保護專業能力之公益社團法人、財團法人及行政法人。	配合本法第五十二條第一項之修正，刪除「行政法人」等文字。
第三十二條 (刪除)	第三十二條 本法修正施行前已蒐集或處理由當事人提供之個人資料，於修正施行後，得繼續為處理及特定目的內之利用；其為特定目的外之利用者，應依本法修正施行後之規定為之。	一、 <u>本條刪除</u> 。 二、現行條文原係配合本法九十九年五月二十六日修正第五十四條所定之過渡條款，旨在強調該次修正前由當事人自行提供之資料，其目的內利用之適法性不受影響。茲考量本法自施行以來，現行公務機關或非公務機關從事蒐集、處理或利用個人資料之行為，已全面適用本法，故本條已無規定之必要，爰予刪除。
第三十三條 本細則施行日期，由 <u>主管機關</u> 定之。	第三十三條 本細則施行日期，由法務部定之。	配合本法修正條文第一條之一主管機關個人資料保護委員會之成立及其監理權限，修正本細則施行日期之指定機關。