

游離輻射設備製造業個人資料檔案安全維護計畫 管理辦法修正總說明

「游離輻射設備製造業個人資料檔案安全維護計畫管理辦法」(以下簡稱本辦法)，於一百零五年二月二十二日發布施行，自發布後未修正。為強化游離輻射設備製造業對個人資料檔案之安全維護管理，依行政院一百十年二月三日「行政機關落實個人資料保護執行聯繫會議」第一次會議決議，及參照一百十年八月十一日行政院發布「行政院及所屬各機關落實個人資料保護聯繫作業要點」，研擬本辦法修正案，其修正重點如下：

- 一、法規名稱酌作文字修正，以資明確。
- 二、修正強化個人資料外洩通報義務。(修正條文第十二條)
- 三、新增強化資訊安全標準規範。(修正條文第十七條)
- 四、新增強化其他安全管理措施。(修正條文第十條、第十一條、第十四條、第十五條、第十六條、第十八條、第十九條、第二十條)

游離輻射設備製造業個人資料檔案安全維護計畫 管理辦法修正條文對照表

修正名稱	現行名稱	說明
游離輻射設備製造業個人資料檔案安全維護管理辦法	游離輻射設備製造業個人資料檔案安全維護 <u>計畫</u> 管理辦法	法規名稱酌作文字修正，以資明確。
修正條文	現行條文	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。	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。	本條未修正。
第二條 本辦法之主管機關為行政院原子能委員會(以下簡稱原能會)。	第二條 本辦法所稱主管機關為行政院原子能委員會。	文字修正。
第三條 本辦法適用對象，指依游離輻射防護法第三十條規定，經營可發生游離輻射設備製造者(以下簡稱業者)。	第三條 本辦法適用對象，指依游離輻射防護法第三十條規定，經營可發生游離輻射設備製造者(以下簡稱業者)。	本條未修正。
<p>第四條 業者應依其業務規模及特性，衡酌經營資源之合理分配，規劃、訂定、檢討、修正及執行個人資料檔案安全維護計畫(以下簡稱<u>安全維護計畫</u>)。</p> <p><u>前項安全維護計畫，應包括下列事項：</u></p> <p>一、個人資料保護政策。</p> <p>二、個人資料之範圍及項目。</p> <p>三、個人資料之蒐集、處理及利用方式。</p> <p>四、個人資料之安全管理及稽核措施。</p> <p>五、個人資料被竊取、竄改、毀損、滅失或洩漏時之通報及應變機制。</p> <p>六、業務終止後其保有個人資料之處理方法。</p> <p>七、對所屬人員之個人資</p>	<p>第四條 業者應依其業務規模及特性，衡酌經營資源之合理分配，規劃、訂定、檢討、修正及執行個人資料檔案安全維護計畫(以下簡稱本計畫)。計畫項目包括：</p> <p>一、個人資料保護政策。</p> <p>二、個人資料之範圍及項目。</p> <p>三、個人資料之蒐集、處理及利用方式。</p> <p>四、個人資料之安全管控、<u>監督</u>及稽核措施。</p> <p>五、個人資料被竊取、竄改、毀損、滅失或洩漏時之通報及應變機制。</p> <p>六、業務終止後其保有個人資料之處置措施。</p> <p>七、對所屬人員之個人資料保護教育訓練。</p>	<p>一、序文酌作文字修正。</p> <p>二、為利閱讀，將序文後段及業者安全維護計畫內容另列為第二項。</p> <p>三、第二項第四款及第六款酌作文字修正。</p>

料保護教育訓練。 八、專責人員及聯絡窗口。	八、專責人員及聯絡窗口。	
<p>第五條 業者申請可發生游離輻射設備之製造許可時，應訂定並檢附<u>安全維護計畫</u>，報請原能會備查；計畫修正時，亦同。</p> <p>業者應自本辦法發布施行之次日起六個月內，完成<u>安全維護計畫</u>之訂定，並報請原能會備查；<u>安全維護計畫</u>因本辦法修正有配合修正必要者，應自本辦法修正施行之次日起六個月內完成修正，並報請原能會備查。</p>	<p>第五條 業者申請可發生游離輻射設備之製造許可時，應訂定並檢附本計畫，報請主管機關備查；計畫修正時，亦同。</p> <p>業者應於本辦法發布施行之次日起六個月內，完成計畫之訂定，並報請主管機關備查。</p>	<p>一、第一項文字修正。</p> <p>二、第二項要求原已訂定安全維護計畫之業者應依本辦法修正其安全維護計畫，並應自本辦法修正施行之次日起六個月內完成修正，並報請原能會備查。</p>
<p>第六條 業者應確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查所保有之個人資料現況。</p> <p>業者經清查發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理、利用之適當處置。</p>	<p>第六條 業者應確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查所保有之個人資料現況。</p> <p>業者經清查發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理或利用等適當之處置。</p>	文字及標點符號修正。
<p>第七條 業者所屬人員為執行業務所蒐集之個人資料，應視為該業者所蒐集持有；於蒐集時，應檢視是否符合蒐集要件及特定目的之必要範圍，並受業者監督。</p>	<p>第七條 業者所屬人員為執行業務所蒐集之個人資料應視為該業者所蒐集持有，於蒐集時應檢視是否符合蒐集要件及特定目的之必要範圍，並接受監督。</p>	<p>明定業者所屬人員執行業務蒐集個人資料之相關行為，應受業者監督，並酌作文字及標點符號修正，以資明確。</p>
<p>第八條 業者與當事人簽訂之委託書，應於委託期限屆至時，主動刪除或銷毀。但因執行業務之必要或經當事人書面同意者，不在此限。</p>	<p>第八條 業者與當事人簽訂之委託書，應於委託期限屆至時主動刪除或銷毀。但因執行業務之必要或經當事人書面同意者，不在此限。</p>	文字及標點符號修正。

<p>業者對當事人刪除或銷毀委託書之請求，認有執行業務之必要者，得不予刪除或銷毀，並應將其理由以書面通知當事人。</p>	<p>業者對當事人刪除或銷毀委託書之請求，認有執行業務之必要，得不予刪除或銷毀，並應將其理由以書面通知當事人。</p>	
<p>第九條 業者委託他人蒐集、處理或利用個人資料之全部或一部時，應於委託契約或相關文件明確約定其內容，並依本法施行細則第八條規定為適當之監督。</p>	<p>第九條 業者委託他人蒐集、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之監督。</p>	<p>明定業者於委託契約或相關文件明確約定對受託者進行蒐集、處理或利用個人資料之監督內容。</p>
<p>第十條 業者就個人資料之蒐集、處理及利用，應符合本法規定，並於安全維護計畫內訂定下列個人資料管理程序：</p> <ol style="list-style-type: none"> 一、蒐集、處理或利用之個人資料包括特種個人資料者，檢視其特定目的及是否符合本法第六條規定。 二、檢視個人資料之蒐集，是否符合本法第八條或第九條應明確告知，或得免為告知之規定；並應明定告知之內容及方式。 三、檢視個人資料之蒐集、處理，是否符合本法第十九條規定之特定目的及法定情形；其經當事人同意者，並應確保符合本法第七條規定。 四、檢視個人資料之利用，是否符合蒐集之特定目的必要範圍；其為特定目的外之利用者，檢視是否符合本法第二十條規定；經當事人同意者，並應確保符合本法第七條規定。 		<ol style="list-style-type: none"> 一、<u>本條新增</u>。 二、要求業者應於第四條安全維護計畫項目第三款，訂定個人資料蒐集、處理及利用之管理程序。

<p>五、利用個人資料行銷，應於首次行銷時，提供當事人免費表示拒絕接受行銷之方式；當事人表示拒絕接受行銷者，應立即停止利用其個人資料行銷。</p> <p>六、進行個人資料國際傳輸前，應檢視有無原能會依本法第二十一條規定所為之限制，並告知當事人其個人資料所欲國際傳輸之區域，同時對資料接收方為下列事項之監督：</p> <p>(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。</p> <p>(二)當事人行使本法第三條所定權利之相關事項。</p> <p>七、當事人行使本法第三條所定權利之相關事項：</p> <p>(一)當事人身分之確認。</p> <p>(二)提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項。</p> <p>(三)對當事人請求之審查方式，並遵守本法有關處理期限之規定。</p> <p>(四)有本法所定得拒絕當事人行使權利之事由者，其理由記載及通知當事人之方式。</p>		
---	--	--

<p>八、維護個人資料正確性，對資料更正、補充、爭議、特定目的消失或期限屆滿、違法蒐集，應依本法第十一條規定辦理。</p>		
<p>第十一條 業者為維護所保有個人資料之安全，應於安全維護計畫內，訂定下列資料安全管理措施：</p> <p>一、訂定各類儲存設備、媒體或資訊系統之使用規範，及安裝設定防毒軟體、防火牆、入侵偵測、漏洞修復、監控機制、帳號管理、存取權限與其他適當防護措施。</p> <p>二、各類儲存設備、媒體或資訊系統報廢或轉作他用時，應採取防範資料洩漏之適當措施。</p> <p>三、對所保有個人資料有加密之需要者，於蒐集、處理或利用時，採取適當之加密措施。</p> <p>四、對所保有個人資料傳輸作業時，採取適當之保護措施。</p> <p>五、對所保有個人資料備份作業過程及所備份之資料，採取適當之保護措施。</p>		<p>一、<u>本條新增</u>。</p> <p>二、要求業者應於第四條安全維護計畫項目第四款，訂定個人資料安全管理措施。</p>
<p><u>第十二條</u> 業者應於安全維護計畫內，訂定應變機制；於發生個人資料被竊取、洩漏、竄改、毀損、<u>滅失</u>或其他侵害事件(<u>以下簡稱事件</u>)時，迅速處理。</p> <p>前項應變機制，應包括下列事項：</p>	<p>第十一條 業者應訂定應變機制，於發生個人資料被竊取、洩漏、竄改或其他侵害事件時，迅速處理。</p> <p>前項應變機制，應包括下列事項：</p> <p>一、採取適當之措施，控制事件對當事人造成之損害。</p>	<p>一、條次變更。</p> <p>二、第一項要求業者應於第四條安全維護計畫項目第五款，訂定個人資料外洩事件之通報及應變機制。</p> <p>三、第二項第二款規定業者設立服務窗口，以增進當事人行使權益之便利</p>

<p>一、採取適當之措施，控制事件對當事人造成之損害。</p> <p>二、查明事件發生原因及損害狀況，以適當方式通知當事人，<u>並設立服務窗口</u>。</p> <p>三、研議改進措施，避免事件再度發生。 業者應自<u>發現事件時起七十二小時內</u>，填列<u>監督通報紀錄表(如附表)</u>通報<u>原能會</u>；並自處理結束之日起一個月內，將處理方式及結果，<u>通報原能會</u>備查。</p> <p><u>原能會接獲前項通報後，得依本法第二十二條至第二十五條規定，對發生第一項事件之業者，為適當之監督管理措施。</u></p>	<p>二、查明事件發生原因及損害狀況，<u>並以適當方式通知當事人</u>。</p> <p>三、研議改進措施，避免事件再度發生。 業者應自事件發生之日起三日內，通報主管機關；並自處理結束之日起一個月內，將處理方式及結果，報主管機關備查。</p>	<p>性。</p> <p>四、第三項為發生個人資料外洩事件之通報時限、對象及方式。</p> <p>五、增訂第四項，原能會接獲前項通報後，得辦理行政檢查，並視檢查結果為後續處置。</p> <p>六、第三項及第四項係依行政院「行政機關落實個人資料保護執行聯繫會議」決議「三、增訂個人資料外洩通報規定」定之。</p> <p>七、酌作文字及標點符號修正。</p>
<p>第十三條 業者業務終止後，<u>不得繼續使用其保有之個人資料，並應於安全維護計畫內，訂定下列處理方式，並留存相關紀錄</u>：</p> <p>一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。</p> <p>二、移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之依據。</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>第十條 業者業務終止後，其保有之個人資料不得繼續使用，得依下列方式處理，並留存相關紀錄：</p> <p>一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。</p> <p>二、移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之<u>合法依據</u>。</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>一、條次變更。</p> <p>二、要求業者應於第四條安全維護計畫項目第六款，訂定業務終止後其保有個人資料之處理方法。</p> <p>三、酌作文字及標點符號修正。</p>
<p>第十四條 業者應於安全維護計畫內訂定教育訓練計畫，定期對所屬人員施以個人資料保護認知宣導及教育訓練。</p> <p>前項認知宣導及教育</p>		<p>一、<u>本條新增</u>。</p> <p>二、要求業者應於第四條安全維護計畫項目第七款，訂定個人資料保護教育訓練。</p>

<p>訓練內容，得包括下列事項：</p> <p>一、個人資料保護相關法令規定、資訊及案例。</p> <p>二、第四條所列安全維護計畫各項管理程序、機制及措施之要求。</p> <p>三、所屬人員之責任範圍。</p>		
<p>第十五條 業者為維護所保有個人資料之安全，應採取下列人員管理措施：</p> <p>一、識別接觸個人資料人員，與相關人員約定保密義務。</p> <p>二、依執行業務之必要，設定相關人員之權限及控管，並定期檢視修正。</p> <p>三、人員離職時，要求返還所保有之個人資料及載體，不得攜離並切結。</p>		<p>一、<u>本條新增</u>。</p> <p>二、要求業者應對保有個人資料之人員採取管理措施。</p>
<p>第十六條 業者保有之個人資料儲存於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦、自動化機器設備或其他媒體者，應採取下列設備安全管理措施：</p> <p>一、依儲存設備或媒體之特性及使用環境，採取適當之保護措施。</p> <p>二、對儲存設備或媒體，訂定適當之保管及管理權限。</p> <p>三、針對存放儲存設備或媒體之環境，實施適當之門禁管制。</p>		<p>一、<u>本條新增</u>。</p> <p>二、因儲存資料之電子設備或媒體具有網路傳輸及可攜帶之特性，為大批個人資料外洩之主要風險途徑，故要求業者應對個人資料儲存設備採取安全管理措施。</p>
<p>第十七條 業者使用資訊服務系統，應採取下列資訊服務安全措施：</p> <p>一、使用者身分確認及保護機制。</p>		<p>一、<u>本條新增</u>。</p> <p>二、依行政院「行政機關落實個人資料保護執行聯繫會議」決議「二、強化資安標準規範」，要求</p>

<p>二、個人資料顯示之隱碼機制。</p> <p>三、網際網路傳輸之安全加密機制。</p> <p>四、個人資料檔案、資料庫之存取控制及保護監控措施。</p> <p>五、防止外部網路入侵對策。</p> <p>六、非法或異常使用行為之監控及因應機制。</p>		業者應加強資訊服務系統資訊安全措施。
<p>第十八條 業者為確保安全維護計畫之落實，應於安全維護計畫內訂定適當之個人資料安全稽核機制，定期或不定期稽核安全維護計畫執行情形，製作稽核報告，並就缺失納入安全維護計畫之檢討修正。</p>		<p>一、<u>本條新增</u>。</p> <p>二、為落實執行成效，要求業者應於第四條安全維護計畫項目第四款，訂定個人資料安全稽核機制。</p>
<p>第十九條 業者為持續精進個人資料安全維護，應參酌執行實務、技術發展、法令變化及其他相關因素，定期檢視或修正安全維護計畫。</p>		<p>一、<u>本條新增</u>。</p> <p>二、要求業者應與時俱進，定期檢視或修正安全維護計畫，以持續精進個人資料安全維護。</p>
<p>第二十條 業者執行安全維護計畫之下列紀錄，至少應保存五年。但其他法令另有規定或契約另有約定者，不在此限：</p> <p>一、個人資料之蒐集、處理及利用紀錄。</p> <p>二、自動化機器設備之軌跡資料。</p> <p>三、執行、稽核或通報等相關報告或紀錄。</p> <p>四、業務終止後之個人資料銷毀、移轉或其他措施之紀錄或證據。</p>		<p>一、<u>本條新增</u>。</p> <p>二、增訂相關文件保存期限。</p>
<p><u>第二十一條</u> 本辦法自發布日施行。</p>	<p>第十二條 本辦法自發布日施行。</p>	條次變更，內容未修正。

第十二條附表修正對照表

修正規定		現行規定	說明
附表 游離輻射設備製造業個人資料外洩事件監督通報紀錄表			一、本表新增。 二、依「行政院及所屬各機關落實個人資料保護聯繫作業要點」，增訂業者通報紀錄表之格式，俾利實務執行。
通報公司名稱： _____ 通報機關： <u>行政院原子能委員會</u>	通報時間： 年 月 日 時 分 通報人： 簽名(蓋章) 職 稱： 電 話： E-mail： 地 址：		
事件發生時間	年 月 日 時 分		
事件發生種類	<input type="checkbox"/> 竊取 <input type="checkbox"/> 洩漏 <input type="checkbox"/> 竄改 <input type="checkbox"/> 毀損 <input type="checkbox"/> 滅失 <input type="checkbox"/> 其他侵害事件	個人資料侵害之總筆數(大約) _____筆 <input type="checkbox"/> 一般個人資料____筆 <input type="checkbox"/> 特種個人資料____筆	
發生原因及事件摘要			
損害狀況			
個人資料外洩可能結果			
擬採取之因應措施			
擬採通知當事人之時間及方式			
是否於發現個人資料外洩後 72 小時內通報	<input type="checkbox"/> 是 <input type="checkbox"/> 否，理由：		