教育部主管目的事業所轄非公務機關
113年度個人資料保護行政檢查計畫

壹、 檢查依據

一、個人資料保護法第27條及個人資料保護法施行細則第12條。

二、行政院及所屬各機關落實個人資料保護聯繫作業要點。

貳、 檢查目的

依個人資料保護法第27條第2項、第3項及個人資料保護法施行細則第12條規定，非公務機關保有個人資料檔案者，應採行適當安全維護措施，防止個人資料外洩，而中央目的事業主管機關亦得指定其所轄管之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。

行政院為落實監管非公務機關個人資料處理作業，由各中央目的事業主管機關就其轄管非公務機關，研提113年度行政檢查計畫，送個人資料保護委員會籌備處（以下簡稱個資籌備處）彙辦。為利本部各事業分組主管司署對所轄非公務機關進行個人資料行政檢查作業有所依循，特訂定本計畫。

參、 評估檢查對象

本計畫檢查對象為本部主管目的事業所轄非公務機關（以下簡稱受檢單位），依本部個資行政檢查小組事業分組，包含：短期補習班、私立兒童課後照顧服務中心。

肆、 非公務機關應遵循之安全維護義務

依「個人資料保護法」第 27 條第 1 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。

伍、 檢查數量

由終身司督導各地方政府針對短期補習班及兒童課後照顧服務中心執行個人資料檔案安全維護行政檢查，主要針對連鎖、具規模、設有系統網站且包含較多個資之業者進行優先檢查，並以書面檢查為原則（不另辦理實地檢查），短期補習班預計檢查30間、兒童課後照顧服務中心預計檢查5間；惟若發生重大個資洩漏案件，各地方政府可視情況進行實地檢查。

陸、作業方式說明

一、 檢查準則及範圍

（一）檢查準則：

1.本部各事業分組主管司署訂定之安維辦法。

2.個人資料保護法及其子法。

3.其他適用之行政院或本部個人資料保護政策或規範。

（二）檢查範圍：

為受檢單位個人資料檔案安全維護計畫所包括之全機關及相關資通系統之各項個人資料保護管理政策、程序等。

二、 檢查方式及項目

（一）實地檢查：

由各事業分組主管司署分析受檢單位之風險程度，或近1至2年內有發生個資外洩之非公務機關，採取風險導向方法選擇辦理實地檢查，檢查項目如表3。

（二）書面檢查：除已實地檢查者，得另辦理受檢單位個人資料檔案安全維護計畫實施情形，或由受檢單位依表3之檢查項　目，並依（三）書面檢查說明辦理。

表 3 檢查項目表[註 1]

項次	檢查項目	檢核細項
1	個人資料檔案安全維護計畫	1.1 訂定「個人資料檔案安全維護計畫」
2	組織及運作管理情形	2.1 指定專人或建立專責組織負責管理
3	專責人員或專責組織任務	3.1 規劃、訂定、修正與執行所訂安維計畫
		3.2 定期向管理人暨代表人或其他代表權人報告
		3.3 依稽核人員評核結果檢討改進，並向管理人與稽核人員提出書面報告

		3.4 訂定個人資料保護管理政策
		3.5 定期對所屬人員進行宣導或專業教育訓練
4	個人資料盤點、管理與紀錄	4.1 定期盤點所保有個人資料並確認應遵守之法令
		4.2 風險分析及管控措施
		4.3 依資料屬性訂定管理程序
		4.4 向當事人蒐集個資，或於利用非由當事人提供之個資前，盡告知義務
		4.5 檢視蒐集、處理個人資料是否符合個人資料保護法第十九條規定之目的及要件
		4.6 委託他人進行資料蒐集、處理或利用，進行適當監督
		4.7 首次利用個資行銷之當事人確認作業
		4.8 確認與維護保有個資之正確性
		4.9 針對所屬人員設定不同管理權限，並要求負保密義務
		4.10 對存有個資之系統設備、媒介物等採取安全管理措施
		4.11 存有個資之系統設備、媒介物報廢或轉作他用時，採取適當防護措施
		4.12 留存所有個資使用紀錄、機關設備軌跡紀錄、相關證據紀錄
5	保有個資達一百筆，或具對外電子商務服務系統[註 2]，或具有特種個資之資通系統之安全管理	5.1 使用者身分確認及保護機制
		5.2 個人資料顯示之隱碼機制
		5.3 網際網路傳輸之安全加密機制
		5.4 個人資料檔案及資料庫之存取控制與保護監控措施
		5.5 防止外部網路入侵對策
		5.6 非法或異常使用行為之監控與因應機制
		5.7 定期演練及檢討改善
6	環境管理措施	6.1 對個資存取媒介物及環境（如機房、雲端），採取環境管理措施
7	業務終止之個資管理	7.1 訂有業務終止之個資處置措施
		7.2 留存相關紀錄
8	事故通報與應變程序	8.1 訂定個資洩漏等事故發生或知悉起 72 小時內通報流程

		8.2 訂定對個資洩漏等事故採應變措施以控制損害
		8.3 訂定查明事故後以適當方式通知當事人之程序並告知已採取因應措施
		8.4 研議預防機制
9	資安檢測	9.1 系統弱點掃描
		9.2 滲透測試
		9.3 資安健診
		9.4 APP 檢測
10	其他[註 3]	

註 1：本表供本部業管單位參考，各業管單位自行依所轄管業者屬性，自行調整項目後提供給受檢單位。

註 2：受檢單位具對外電子商務服務系統方須填寫。

註 3：由本部業管單位依其他規範，自行訂定。

三、 書面檢查說明

（一）受檢單位收到事業分組主管司署或地方政府函文，依函文交付期限內填具查核表（含單位基本資訊），將查核表與佐證資料寄至各主管司署或地方政府指定信箱，或至指定系統填報並上傳佐證資料。

（二）各事業分組主管司署或地方政府收到受檢單位查核表與佐證資料，就所提交之資料邀請書面審查委員提供建議與意見。

（三）非公務機關由地方政府主管之查核對象，由該非公務機關主管司署或地方政府邀請具實務專業之公務機關代表或專家學者辦理。

四、 實地檢查說明：

（一）由各事業分組主管司署領隊帶領檢查團隊至受檢單位進行實地檢查。

（二）實地檢查時間將依受檢單位業務複雜度、辦公場域數量、蒐集處理利用個資數量等因素，彈性調整檢查時程。檢查啟始/結束會議之受檢單位代表建議由各事業別主管司署個資管理人（如個資長或資安長）或如有委由地方政

府辦理者，由地方政府派員，以帶領受檢單位之個資管理及追蹤改善。

（三）非公務機關由地方政府主管之受檢單位，由該非公務機關主管司署或地方政府派員辦理，本部得派員參與。

柒、 受檢查業者配合事項

一、 本部各事業分組主管司署或地方政府於檢查前 1 個月通知受檢單位，並請受檢單位於文到後 2 週內填復查核表與佐證資料，俾利檢查團隊辦理作業。

二、 本計畫查核表由本部依最新法令要求、各事業別安維辦法及重大個資政策制定，前述查核表可由本部各事業分組依受檢單位業務性質差異等情形進行滾動修正，如有更新情形，本部將於適用該查核表之受檢單位時程前 1 個月公告周知。

三、 請受檢單位於實地檢查前，提供單位最新版之「個人資料檔案安全維護計畫」、「個資檔案盤點清冊」，及「最近一次管理審查會議紀錄」，俾利檢查團隊初步瞭解該機關個人資料檔案安全維護計畫實施情形。

四、 本部統籌辦理行政檢查說明會，其辦理時程、地點及相關事項將另行通知。

捌、 檢查後處理方法

一、 本部各事業分組主管司署或地方政府將於每年度檢查結束後，就受檢單位未完成檢查項目，自行本於權責管考及輔導受檢單位, 提供管制表並定期追蹤受檢單位，受檢單位就未完成之項目研議因應作為及辦理時程，定期填報並回復本部各事業分組主管司署或地方政府。

二、 若書面檢查或實地檢查中發現受檢單位疑似有個資外洩情況發生，請本部各主管事業司署依「行政院及所屬各機關落實個人資料保護聯繫作業要點」規定，於知悉個資外洩 72 小時內填列監督通報紀錄表，並通報個資籌備處。

三、 各年度個資行政檢查作業結束後，將彙整所有受檢單位檢查結果，並提出檢查共同發現事項及建議，供本部主管事業司署參考改進。