國家通訊傳播委員會
個人資料保護與管理法遵文件
V1.1

財團法人資訊工業策進會

中華民國107年07月

目 錄

表 目 錄

壹、國家通訊傳播委員會轄下業者個人資料保護與管理自我評核表

表 1 填寫說明表

基本資料列暨填寫說明			
廠商名稱		填表日期	

資料來源：本計畫自行製表

【國家通訊傳播委員會轄下業者個人資料保護與管理自我評核表說明】

個人資料保護與管理自我評核表（以下簡稱本表），係為國家通訊傳播委員會（以下簡稱通傳會）委託財團法人資訊工業策進會制定，以推動通傳會業者（以下簡稱業者）營運之個人資料保護與管理基本防護查核，以引導業者建立自主個人資料保護與管理。

■ 目的：

本表旨在提供業者個人資料保護與管理之基礎要求，以協助並引導業者因應法規要求與建立個資保護與管理參考。本表係引導並鼓勵業者自主管理之建議性質，業者可參考本自我評核表，但不以此為限，以考量業者營運風險與需求，訂定符合業者本身營運需求之個人資料保護與管理制度。

■ 使用對象：

通傳會所管理之通訊傳播業者。

■ 如何使用本表：

本表係依據個人資料保護法、施行細則，以及通傳會於 105 年 11 月 9 日通傳平臺字第 10541037790 號，頒佈之「國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法」(下載網址：https://www.ncc.gov.tw/chinese/law_detail.aspx?site_content_sn=502&law_sn=2575&sn_f=2575&is_history=0)，之規定，依序展開個人資料保護與管理之控制措施，並提供導入時之說明及參考資料。

本表宜由負責**業務主管**、**法務**與**相關管理人員**，共同填寫本表，以使相關管理者對個人資料保護與管理措施有更深入了解，並促進管理與法律之協同管理。填寫步驟如下：

一、 依序由第 1 題填寫至第 13 題，以本表之查核內容為基準，並可參考「說明及參考資料」欄位，瞭解本查核項之具體內容或程序文件

範例，比對業者本身現行個人資料保護與管理措施作法，將比對後之結果作為判斷之依據，擇一勾選符合程度（「是」/「否」/「不適用」欄位，並將相關證明文件、紀錄及說明填寫於填寫於「提出佐證證明或說明」欄位。

二、 本表後附有「個人資料保護法」、「個人資料保護法施行細則」，及「國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法」供業者查詢參考。

三、 填寫範例如下：

表 2 填寫範例表

查核項目	查核內容	查核結果	提出佐證證明或說明	說明及參考資料	因應條文說明
9. 個人資料業務委外	本組織是否針對個人資料委外業務，依照個資法規定予以監督管理？	■是 □否 □不適用	詳附件： **委外監督管理程序、監督管理紀錄表** **XXX 廠商契約** 說明： **本組織設置委外監督管理程序，並簽訂委外契約，且每年至少一次對委外廠商監督管理。**	**【說明】** 組織有依個資法（施行細則第 8 條），善盡對受託組織之監督，以確保受託組織有依照組織之要求執行業務？ **【佐證證明或說明參考範例】** 如：個人資料委外處理管理程序、委外契約，或委外監督管理紀錄等。 **【參考資料】** 參考指引 貳、八、【業務委外】某購物平台業者 G 將快遞業務委由物流業者 H 執行，G 該如何善盡監督責任？ 個人資料委外處理管理程序（範例）	個資法第 4 條 施行細則第 7、8 條 安全維護辦法第 5 條第 1 項第 6 款

資料來源：本計畫自行製表

四、 業者可參考「說明及參考資料」欄位中之【說明】，以瞭解本項目欲查核內容，【佐證證明或說明參考範例】則能知悉前欄位可提出證明或說明之範例，【參考資料】之參考指引或程序文件（範例），做為內部建置個人資料保護與管理制度之依據，若具體執行內容有需進一步協助或瞭解之處，可洽臺灣個人資料保護與管理制度諮詢服務網頁（https://www.tpipas.org.tw/privacy.aspx?b=y），將由專人提供相關諮詢服務。

國家通訊傳播委員會轄下業者個人資料保護與管理自我評核表

表 3 自我評核表

自我評核表內容					
查核項目	**查核內容**	**查核結果**	**提出佐證證明或說明**	**說明及參考資料**	**因應條文說明**
1. 法律責任	本組織清楚瞭解，違反個人資料保護法將有可能遭到民事損害賠償的請求，及刑事或行政處分的處罰。	□ 是 □ 否	詳附件： 說明：	**【說明】** 違反個資法，可能受到之處罰，可參考個資法第 25、26、28、41、42、47~50 條等規定。 **【佐證證明或說明參考範例】** 如：員工工作規範、組織教育訓練內容或相關公告有說明相關法律責任。 **【參考資料】** 參考指引 壹、 三、【法律風險】蒐集個資的組織或個人是否可以不遵守個資法的規範？	個資法第 28、41、42 及 47~第 50 條
2. 投入資源與人力	本組織是否有投入必要的資源與人力，以維持內部個人資料保護與管理能力。	□ 是 □ 否	詳附件： 說明：	**【說明】** 組織已投入適當教育訓練、擇定人員執行個人資料保護、編定個資保護法遵文件或建置個人資料保護與管理制度以保障個資安全。 前開文件或制度之簽署，應由負責人或法定代理人為之。 **【佐證證明或說明參考範例】** 如：個資保護小組組織架構圖、個資保護管理政策等	施行細則第 12 條第 2 項第 1 款 安全維護辦法第 3 條
3. 界定個人資料	本組織是否有針對含有個人資料之業務進行個資盤點？	□ 是 □ 否	詳附件： 說明：	**【說明】** 組織已清點所有含有個人資料之流程或檔案，並保留相關紀錄。 **【佐證證明或說明參考範例】** 如：個資盤點表、流程圖，或個資清冊。	施行細則第 12 條第 2 項第 2 款

自我評核表內容					
查核項目	**查核內容**	**查核結果**	**提出佐證證明或說明**	**說明及參考資料**	**因應條文說明**
				【參考資料】 個人資料盤點管理程序（範例）	
4. 風險評估	本組織是否有針對含有個資之流程進行風險評估？	□ 是 □ 否	詳附件： 說明：	**【說明】** 組織已針對所有含有個人資料之流程或檔案，評估可能發生個資事故的風險並採取必要之改善措施。 **【佐證證明或說明參考範例】** 如：風險評估管理程序、風險評估表，或針對高風險流程所採取控制措施之紀錄。 **【參考資料】** 個人資料風險評估管理程序（範例）	施行細則第 12 條第 2 項第 3 款
5. 事故通報應變	本組織針對個資事故是否設有通報及應變程序？	□ 是 □ 否	詳附件： 說明：	**【說明】** 組織已針對個資事故之發生，設置必要的應變機制，如應變小組、應變方式及追蹤改善措施等，以降低個資事故造成之影響。 應變方式包含查明事故後以適當方式通知當事人，及遇重大個資事故時，應即通報通傳會等內容。 **【佐證證明或說明參考範例】** 如：個人資料事故緊急應變管理程序、事故通報單，或可具體說明事故處理方式等。 **【參考資料】** 參考指引 貳、十一、【人員管理】某電信業者Ｖ該如何降低員工因故意或過失而引起之個資外洩事故？ 個人資料事故緊急應變處理程序（範例）	個資法第 12 條 施行細則第 12 條第 2 項第 4 款 安全維護辦法第 4 條

自我評核表內容					
查核項目	**查核內容**	**查核結果**	**提出佐證證明或說明**	**說明及參考資料**	**因應條文說明**
6. 蒐集處理利用之內部管理程序	6.1 本組織資料蒐集、處理是否符合個資法之法定要件？	□ 是 □ 否	詳附件： 說明：	**【說明】** 組織蒐集、處理個人資料，皆能有適當之蒐集目的，以及合法之法定情形。 **【佐證證明或說明參考範例】** 如：蒐集、處理或利用管理程序、蒐集、處理或利用審核表，或審核紀錄等。 **【參考資料】** 參考指引 貳、一、【個資蒐集】某電信業者 A 組織，希望藉由大量的用戶資料，作為其行銷的對象，請問該如何才能合法蒐集個人資料？	施行細則第 12 條第 2 項第 5 款 安全維護辦法第 5 條第 1 項第 3 款
	6.2 本組織蒐集當事人個資是否有依法履行告知義務？	□ 是 □ 否 □ 不適用	詳附件： 說明：	**【說明】** 組織於蒐集個資時，有確實執行告知當事人依法應說明的事項，或是有明確依法得免告知的事由（如有則勾選「不適用」，並於說明欄位敘明免告知之法定情形）。 **【佐證證明或說明參考範例】** 如：蒐集個資流程之告知函或告知紀錄。 **【參考資料】** 參考指引 貳、二、【告知義務】某有線電視業者 B 向消費者/員工蒐集了個人資料，該如何向其履行個資法之告知義務？	個資法第 8 條 第 5 條第 1 項第 2 款
	6.3 本組織利用個人資料是否都符合個資法要求？	□ 是 □ 否	詳附件：	**【說明】** 組織有判斷哪些作業流程有利用個資，並於原蒐集個資之特定目的內利用個人資料，如有特定目的外	個資法第 20 條第 1 項 施行細則第 12 條第 2 項第 5 款

自我評核表內容					
查核項目	查核內容	查核結果	提出佐證證明或說明	說明及參考資料	因應條文說明
			說明：	利用個資之情形，確保皆有符合法定情形，如係經當事人同意者，並應確保有取得當事人之明示同意。。 **【佐證證明或說明參考範例】** 如：蒐集、處理及利用管理程序、利用個資之審核表，或審核紀錄。 **【參考資料】** 參考指引 貳、三、【個資利用】某電視購物業者 C 可否將員工或會員的資料轉賣給其他組織？	第 5 條第 1 項第 4 款
	6.4 本組織是否有符合個資法行銷相關規定？	□ 是 □ 否 □ 不適用	詳附件： 說明：	**【說明】** 組織於執行行銷業務時，有提供當事人表示拒絕行銷之管道，並確實落實避免針對前述當事人再次行銷之方法。倘組織並無利用個人資料進行行銷之情形，則可勾選「不適用」。 **【佐證證明或說明參考範例】** 如：行銷處理辦法，或當事人行使拒絕行銷之紀錄。 **【參考資料】** 參考指引 貳、五、【行銷活動】某電信業者 D 是否可向消費者發送行銷訊息，或組織出版刊物？	個資法第 20 條第 2、3 項 安全維護辦法第 5 條第 1 項第 5 款
	6.5 本組織於蒐集、處理或利用過程中，是否能確保個人資料之正確性，並就不正確或正確性有爭議之資料，有適當之處置方式？	□ 是 □ 否	詳附件： 說明：	**【說明】** 組織於蒐集、處理或利用個資時，是否能有適當方式確保個人資料之正確性，並主動或依當事人之請求補充或更正之。 但如個資之正確性有爭議，則應主動或依當事人之	個資法第 11 條第 1、2 及第 5 項 安全維護辦法第 5 條第 1 項第 9 款

自我評核表內容					
查核項目	查核內容	查核結果	提出佐證證明或說明	說明及參考資料	因應條文說明
				請求，刪除、停止處理或利用該個資。但因執行職務或業務所必須或經當事人書面同意者，不在此限。 **【佐證證明或說明參考範例】** 如：蒐集、處理或利用審核表、審核紀錄、當事人權利行使管理程序、權利行使申請表，或審核紀錄等。	
	6.6 本組織就特定目的消失或期限屆滿之個人資料，能依個資法進行刪除、停止處理、利用該個資等相關處置方式？	□ 是 □ 否	詳附件： 說明：	**【說明】** 組織就特定目的消失或保存期限屆滿之個人資料，皆能刪除、停止處理或利用該個人資料。 **【佐證證明或說明參考範例】** 如：蒐集、處理及利用管理程序、資料刪除、銷毀管理程序，或資料刪除、銷毀之紀錄等。 **【參考資料】** 參考指引 貳、七、【客戶服務】消費者乙要求某電信業者 F 刪除其個人資料，F 該如何處理？	個資法第 11 條第 3 項 安全維護辦法第 5 條第 1 項第 10 款
7. 特種個人資料	本組織是否有依個資法規定蒐集、處理或利用特種個人資料（病歷、醫療、健康檢查、基因、犯罪前科、性生活）？	□ 是 □ 否 □ 不適用	詳附件： 說明：	**【說明】** 組織有明確之法令依據，以合法蒐集特種個人資料。如組織並未蒐集、處理或利用特種個人資料，則可勾選「不適用」。 **【佐證證明或說明參考範例】** 如：蒐集、處理及利用管理程序、法令盤點表（有針對是否得蒐集、處理或利用特種個資予以審核），或審核紀錄。	個資法第 6 條 安全維護辦法第 5 條第 1 項第 1 款

自我評核表內容					
查核項目	查核內容	查核結果	提出佐證證明或說明	說明及參考資料	因應條文說明
				【參考資料】 參考指引 貳、四、【人力資源】人資專員甲是否可以向員工蒐集健康檢查、警察刑事紀錄證明書（良民證）等資料？又如果警調來函要求醫院配合案件調查提供某病患病歷，應該提供嗎？	
8. 當事人權利行使	本組織是否有提供當事人針對其個人資料，行使查詢、閱覽、請求製給複製本，要求停止或刪除其個人資料之權利？	□ 是 □ 否	詳附件： 說明：	**【說明】** 組織有明確的管道以便當事人行使其權利，並能於個資法規定（第 13 條）之期限內完成對當事人請求之答覆。 組織並設置聯絡窗口以供當事人申訴或諮詢。 **【佐證證明或說明參考範例】** 如：當事人權利行使管理程序、權利行使申請表，或審核紀錄。 **【參考資料】** 參考指引 貳、七、【客戶服務】消費者乙要求某電信業者 F 刪除其個人資料，F 該如何處理？	個資法第 3、13 及第 14 條 安全維護辦法第 5 條第 1 項第 8 款、第 11 款
9. 個人資料業務委外	本組織是否針對個人資料委外業務，依照個資法規定予以監督管理？	□ 是 □ 否 □ 不適用	詳附件： 說明：	**【說明】** 組織有依個資法（施行細則第 8 條），善盡對受託組織之監督，以確保受託組織有依照組織之要求執行業務。如組織並無將含有個人資料之業務委託其他組織、個人執行，則可勾選「不適用」。 **【佐證證明或說明參考範例】** 如：個人資料委外處理管理程序、委外契約，或委外監督管理紀錄等。	個資法第 4 條 施行細則第 8 條 安全維護辦法第 5 條第 1 項第 6 款

自我評核表內容					
查核項目	查核內容	查核結果	提出佐證證明或說明	說明及參考資料	因應條文說明
				【參考資料】 參考指引 貳、八、【業務委外】某電視購物業者 G 將快遞業務委由物流業者 H 執行，G 該如何善盡監督責任？ 個人資料委外處理管理程序（範例）	
10. 個人資料之國際傳輸	本組織將個人資料進行國際傳輸，是否符合個資法及通傳會之規定？	□ 是 □ 否 □ 不適用	詳附件： 說明：	**【說明】** 組織於進行個人資料國際傳輸時，並無違反個資法第 21 條，及通傳會以法規或命令禁止之情形者。如組織經確認後，並無將個人資料進行國際傳輸之情形，則可勾選「不適用」。 **【佐證證明或說明參考範例】** 如：個人資料跨境傳輸管理程序。 **【參考資料】** 參考指引 貳、九、【國際傳輸】某電信業者 H 可否將含有個人資料的檔案傳送至國外的部門、分公司或是合作飯店？	個資法第 21 條 安全維護辦法第 5 條第 1 項第 7 款
11. 資訊安全	本組織是否依照需求，建置適當的管控措施，以確保資訊安全的要求？	□ 是 □ 否	詳附件： 說明：	【說明】 組織是否針對重要之流程、部門或全公司、全業務流程，建置資訊安全防護措施，以降低個資外洩之風險。 【佐證證明或說明參考範例】 如：通過並有效之 ISO27001 驗證、資訊安全管控程序等。	施行細則第 12 條第 2 項第 6 款、第 8 款

自我評核表內容					
查核項目	**查核內容**	**查核結果**	**提出佐證證明或說明**	**說明及參考資料**	**因應條文說明**
12. 認知宣導與教育訓練	本組織會定期針對新進人員及內部員工施以個資保護與管理相關教育訓練，以培養其個資保護之意識與能力？	□ 是 □ 否	詳附件： 說明：	**【說明】** 組織針對員工進行定期（每年至少一次）之個人資料保護與管理之教育訓練，並針對專責人員提供進階教育訓練，以培養組織內部個資保護專人。 **【佐證證明或說明參考範例】** 如：教育訓練程序、教育訓練教材、教育訓練紀錄，或宣導資料等。	施行細則第 12 條第 2 項第 7 款
13. 稽核機制	本組織是否定期針對業務執行情形予以稽核、查檢，以確保符合個資法及內部規範要求？	□ 是 □ 否	詳附件： 說明：	**【說明】** 組織定期（每年至少一次）依照個資法及內部個人資料保護與管理相關程序、辦法之規定，確認內部人員是否如實執行相關要求。 如所蒐集之個資達五千筆以上，應包含國內或國際個人資料安全稽核機制之規劃或執行計畫。 **【佐證證明或說明參考範例】** 如：稽核紀錄。 參考指引 貳、十三、【稽核改善】組織該如何確保所建置之管理制度係正常運作且能持續改善？	施行細則第 12 條第 2 項第 9 款 安全維護辦法第 3 條第 3 項
14. 紀錄保存	本組織是否保存個資管理紀錄、軌跡資料或證據？	□ 是 □ 否	詳附件： 說明：	**【說明】** 相關紀錄、軌跡資料或證據，如：特定目的外利用審核、當事人權利行使紀錄及個人資料檔案刪除/銷毀、委外監督紀錄等。 **【佐證證明或說明參考範例】** 如：各程序之保留紀錄，例：刪除/銷毀管理程序或銷毀紀錄等。	施行細則第 12 條第 2 項第 10 款 安全維護辦法第 6 條

國家通訊傳播委員會轄下業者個人資料保護與管理自我評核表

自我評核表內容					
查核項目	**查核內容**	**查核結果**	**提出佐證證明或說明**	**說明及參考資料**	**因應條文說明**
15. 持續改善	本組織是否定期執行個人資料安全維護與管理之整體持續改善？	□ 是 □ 否	詳附件： 說明：	**【說明】** 組織確實針對稽核之結果、法規之變更、主管機關或業主之要求等情形，改善組織個人資料保護與管理制度之作法，以持續改善內部個資保護力。 **【佐證證明或說明參考範例】** 如：針對稽核、缺失或主管機關、業主所提出改善建議所執行修正之紀錄。 參考指引 貳、十三、【稽核改善】組織該如何確保所建置之管理制度係正常運作且能持續改善？	施行細則第 12 條第 2 項第 11 款
填表人		**聯絡電話**		**電子郵件**	

資料來源：本計畫自行製表

貳、國家通訊傳播委員會轄下事業個人資料保護與管理法遵文件參考指引

內容

壹、基礎認知篇

一、【基本目的】什麼是個人資料保護法？它的目的是什麼？

1. 說明：

由於電腦科技進步迅速，網際網路、雲端服務及大數據等新運用型態的蓬勃發展，除了帶給人民便捷的生活與經濟的發展外，同時也增加了個人資料遭到濫用的可能性，我國於民國 84 年制定電腦處理個人資料保護法，希望藉由參考經濟合作暨發展組織（OECD）針對個人資料自動化處理公約所提出之八大原則，以及師法日本、德國國內對於個資保護之立法，加強我國就電腦處理個人資料之保護。

而為了擴大個資保護的範圍，我國亦於民國 99 年制定個人資料保護法（以下簡稱個資法），本法保護客體除了不再限於電腦處理之個人資料外，更加強規範個資蒐集、處理及利用之行為，而本法於民國 104 年再次修正，以使個資法更能順應社會之需求。

因此，個人資料保護法係一部無論是組織或個人，公務或非公務機關，於蒐集、處理或利用個人資料時，皆應恪遵之法典準繩，除了保障當事人個資及隱私權之外，亦能促進個人資料之合理利用。

2. 參考資料：

- 電腦處理個人資料保護法（84 年 7 月 12 日制定、84 年 8 月 11 公布）第 1 條。
- 個人資料保護法（99 年 5 月 26 日公布、101 年 10 月 1 日施行）第 1 條。
- 個人資料保護法（104 年 12 月 30 日公布、105 年 3 月 15 日施行）第 1 條。

二、【基本原則】組織在蒐集消費者或是員工的個資時，是否可以毫無限制、竭盡可能地蒐集大量個資，以備日後不時之需？

1. 說明：

依個資法要求，個人資料之蒐集、處理或利用，應與蒐集之目的有合理正當之關連性，且不得與其他目的作不當連結，因此組織於蒐集個人資料時，可掌握以下原則：

- 僅蒐集最小、必要之個人資料欄位，避免過度蒐集，侵害當事人權利，並增加管理上之風險（例：如某客服 M 應徵電話客服員，卻要求員工體檢需提供梅毒血清檢驗）。

2. 參考資料：

- 個人資料保護法第 5 條。

三、【法律風險】蒐集個資的組織或個人是否可以不遵守個資法的規範？

1. 說明：

對於違反個資法的組織，除了商譽或形象會遭受到嚴重的影響，以及民事損害賠償、行政處分或罰鍰，個人甚至可能會被判處有期徒刑、拘役、科或併科罰金，而且截至目前，業有為數相當的組織及個人遭到法規的制裁，現以下表說明公務或非公務機關違反個資法可能會產生的法律風險，

並顯示出無論係組織或個人，遵守個資法並降低法律風險，皆有其必要性：

公務或非公務機關違反個資法規定之民事損害賠償			
機關別	**賠償責任**	**賠償金額**	**最高賠償總額**
公務機關	除因天災、事變或其他不可抗力所致者，其他皆須負擔損害賠償責任 （第 28 條第 1 項：無過失責任）	如受害者無法證明其實際損害額時，得請求以每人每一事件新臺幣 5 百元以上 2 萬元以下計算 （第 28 條第 3 項）	以新台幣 2 億元為限 （第 28 條第 4 項）
非公務機關	如能證明係非故意或過失，則無須負擔損害賠償責任 （第 29 條：舉證責任倒置）		

公務機關違反個資法規定之刑事與行政責任				
違反事項		**刑事責任**	**行政責任**	**備註**
第 15 條	公務機關違反蒐集、處理之特定目的、法定情形之規範	（第 41 條） 五年以下有期徒刑，得併科新臺幣一百萬元以下罰金	其他公務員應遵守之行政法規	（第 44 條） 公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一
第 16 條	公務機關違法利用或特定目的外利用個資			
第 42 條	意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者	五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金		

非公務機關違反個資法規定之刑事與行政責任				
違反事項		**刑事責任**	**行政責任**	**備註**
第 6 條 第 1 項	特種個資之蒐集、處理或利用	（第 41 條） 五年以下有期徒刑，得併科新臺幣一百萬元以下罰金	（第 47 條） 新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之	（第 50 條） 非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者
第 19 條	非公務機關違反蒐集、處理之特定目的、法定情形之規範			
第 20 條 第 1 項	非公務機關違法利用或特定目的外利用個資			

第 21 條	國際傳輸限制			外，應並受同一額度罰鍰之處罰
第 8、9 條	直接/間接告知義務	N/A	（第 48 條） 命限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰	
第 10、11、12 條	當事人權利行使通知義務			
第 20 條 第 2、3 項	個人資料行銷			
第 27 條第 1 項、第 2 項	未採行適當之安全措施，未採行中央目的事業主管機關指定之非公務機關訂定個人資料檔案安全維護辦法或業務終止後個人資料處理方法			
第 22 條 第 4 項	規避、妨礙或拒絕中央目的事業主管機關之行政檢查		（第 49 條） 新臺幣二萬元以上二十萬元以下罰鍰	
第 42 條	意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者	五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金	依個案違法事實，亦有可能違反本法第 27 條第 1 項支規定	N/A

貳、 組織與個資

一、【個資蒐集】某電信業者 A 公司，希望藉由大量的用戶資料，作為其行銷的對象，請問該如何才能合法蒐集個人資料？

1. 說明：

對於無論公務或是非公務機關，蒐集個人資料幾乎都是必要的業務內容，但是如果要合法的蒐集個人資料，可以參考以下重點，

- ◆ 應確保有合理之蒐集目的：如係基於人事管理之目的蒐集公司員工個資，或是基於消費者服務與管理之目的，蒐集客戶個資等。
- ◆ 應有符合個資法要求之法定情形：簡而言之，便是蒐集個資需有合法之理由，一般而言組織較常使用之法定情形為與當事人有契約或類似契約之關係，且已採取適當之安全措施，如與員工簽署之勞動契約，與消費者訂定之買賣契約，皆可適用於本情形。而其他法定情形如在網站或一般可得的資源中所取得之個資，亦會發生在組織舉辦會議，邀請專家學者時，可能會先至網站搜尋其學經歷等情形，但如果都沒有相關適切之法定情形，亦可經由取得當事人同意，合法蒐集其資料。
- ◆ 確保能符合個資蒐集之必要性及最小性原則：以往組織之習慣，皆希望能從員工或消費者身上汲取越多個人資料，以期能更了解自己的員工，及洞悉消費者的消費習慣等，但在現今個資保護意識抬頭的年代，為了降低組織管理個資之風險，摒棄過往過度蒐集個資之習慣，亦為應調整之觀念。
- ◆ 於蒐集個資後，應履行告知義務（詳細內容可見下一問）。

2. 參考資料：

- ◆ 公務機關：個資法第 15 條。
- ◆ 非公務機關：個資法第 19 條。
- ◆ 個資法第 5 條。

二、【告知義務】某有線電視業者 B 向消費者/員工蒐集了個人資料，該如何向其履行個資法之告知義務？

1. 說明：

為了保護當事人個資安全，並尊重其隱私權，組織在蒐集個資前，皆應使個資當事人明確瞭解其個人資料將被或已被蒐集、處理以及利用等相關的情形，可使其有機會預先判斷這些個資行為是否合法，以及自己是否可以接受蒐集者的處理方式，並且可以使當事人及早採取相關因應與救濟措施，以降低損害的情形及預防個資遭到不法或不當濫用，因此組織對於踐行告知義務，應注意以下事項：

- ◆ 是否完整清查所有蒐集個資之流程或作業：唯有確認過組織所有蒐集個資之流程後，才能完整逐一進行告知，以免因為一時疏忽，漏未進行告知。
- ◆ 確認蒐集個資之流程或作業是否有符合免告知之法定情形：個資法原則上要求蒐集個資之組

織或個人，皆應履行告知義務，僅於例外之情形，才能免除告知義務，因此組織亦可於告知前檢核是否有得免告知之法定情形，如有法定免告知事由，如保險業為執行核保或理賠作業需要，處理、利用保險契約受益人之個資，得免為個資法之告知間接蒐集個資，或該個資係因當事人自行公開或其他已合法公開之個人資料，如於網路上搜尋取得，或公司負責人資料等依法應公開之個資等。

- 告知之方式：個資法並未具體要求組織於告知當事人應採取之方式，只要足以使當事人知悉或可得知悉之方式即可，並不以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件等方式為限。
- 告知函範本：

一、 蒐集個資之機關名稱。

（如：XXX 股份有限公司）

二、 蒐集之目的。

（如：基於消費者服務、商品販售、貨物宅配之目的）

三、 個人資料的類別。

（如：姓名、聯絡電話、住址、信用卡號碼、銀行帳戶）

四、 個人資料利用之期間、地區、對象及方式。

（如：本資料將會使用於消費者及客戶服務與管理之目的，用作消費者與客戶聯繫溝通之用，以及作為本公司行銷之用，而使用於中華民國境內，並會保留 15 年後刪除之。）

五、 當事人依第 3 條規定得行使之權利及方式。

（例：如欲行使當事人權利，可於本所週一至週五上班時間（09:00~18:00）撥打免付費電話 0800-000-000，將有專人為您服務）

六、 當事人得自由選擇提供個人資料時，不提供將對其權益造成之影響。

（例：如您不提供或拒絕提供正確的個資，將無法使用本公司購物之服務）

註：如資料係非由當事人直接提供者（間接蒐集），則應向當事人告知個資取得之來源，以及前條第 1 項至第 5 項之內容。

（如：您的資料係由 XXX 單位提供取得）

2. 參考資料：
   - 直接蒐集告知：個資法第 8 條。
   - 間接蒐集告知：個資法第 9 條。
   - 保險核保或理賠免告知：保險法第 177-1 第 3 項。
   - 告知之方式：個資法施行細則第 16 條。

三、【個資利用】某電視購物業者 C 可否將員工或會員的資料轉賣給其他組織？

1. 說明：

組織於所保有之個人資料檔案，有時會希望或被要求做原蒐集特定目的外之利用（如轉賣、提供給檢警調或其他組織等），因個資的當事人，往往無法預期這一類目的外利用的情形發生，因此容易對其個資產生比較大的影響，是故組織如欲將資料作特定目的外利用，應注意以下重點：

- 是否有符合個資法規範之法定情形：於個資法規範下，原則係禁止為特定目的外利用，僅在例外的情形下方可利用之，如悠遊卡公司將悠遊卡刷卡交易相關資料提供予公務機關，作為協助其執行規劃與管理大眾運輸系統之用途，即可認做符合「為增進公共利益」之法定情形，而得合法提供。
- 如係經當事人同意：組織應注意需向當事人明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示，如於書面申請單上獨立標示出特定目的外利用之說明項目，並請當事人詳閱後簽名表示同意之。另外需特別留意的是，組織應避免採取「預設同意」的方式取得當事人同意，亦即消費者於提供資料時，如未明確表示拒絕接受其他合作企業之行銷資訊，則視為同意的意思表示等情形。
- 合理正當關聯性：儘管於特定目的外利用法定情形之評估下，係符合個資法規範，但仍須注意目的外利用之範圍仍應與原蒐集特定目的具有合理正當關聯性，並以必要性為原則。
- 保留必要紀錄：如前（壹、三）所述，因組織需負擔證明其非故意或過失，因此於執行特定目的外利用之業務時，應保留必要之紀錄，如機關來函調閱資料之公文、組織內部審核是否提供個資之紀錄等，以作為後續降低法律風險之證據。

2. 參考資料：

- 特定目的外利用：個資法第 16、20 條。
- 悠遊卡提供資料：法務部 103 年 6 月 26 日法律字第 10303507480 號函釋。
- 經當事人同意：個資法第 7 條第 2 項、施行細則第 15 條。
- 合理正當關聯性：個資法第 5 條。
- 舉證責任倒置：個資法第 29 條。

四、【人力資源】人資專員甲是否可以向員工蒐集健康檢查、警察刑事紀錄證明書（良民證）等資料？又如果警調來函要求醫院配合案件調查提供某病患病歷，應該提供嗎？

1. 說明：

組織為符合法令規範，或基於營運之考量，有時需向員工蒐集如健康檢查、警察刑事紀錄證明書，或信用紀錄等，但這些個人資料往往具有高度的隱私保護性，如果外洩，將會對個人造成重大危害。因此組織於蒐集、處理或利用這些資料，便需提供更完善的保護與管理，及重視以下原則：

- 何謂特種個資：病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，因係高度敏感之個資，故個資法針對這些資料予以特殊保護。而各國之間針對風土民情之差異，亦對於

特種（敏感）個資的認定有所差異，如英國所定義之敏感性個資為種族、政黨傾向、宗教信仰、加入之貿易聯盟、身體或心理之健康或狀態、性生活、任何確定或疑似犯罪之行為、任何法庭正在處理之確定或疑似犯罪之行為的處理程序與判決或歐盟通用資料保護規則（GDPR）所定義之敏感資料為種族、政治意見、宗教、哲學信仰、參與工會、基因、生物特徵資料、有關健康的資料、性生活或性取向。

- 蒐集、處理或利用特種個資之法定情形：個資法為針對當事人特種個資的保護，原則上為禁止，例外僅有在符合法定情形之條件下才可為使用。如組織基於法律規範，雇主於雇用勞工時，應施行體格檢查，並應保存該檢查紀錄，於此即係符合個資法基於「非公務機關履行法定義務必要範圍內」，得例外蒐集、處理或利用健康檢查報告。

  於此應特別注意者，惟部分組織基於提供員工福利之前提，會提供員工接受超過一般體格檢查之較高規格健檢，便需留意應考量是否請醫院僅提供法令規定之必要檢查項目報告與組織即可，較完整之報告內容，僅由員工保留，才可有效降低個資風險，又能達到公司提供福利之目的。

  倘組織係基於「經當事人書面同意」而取得，則亦需注意是否有逾越特定目的必要範圍、法律另有限制，或其同意違反其意願等情形，如某研究機構欲以某原住民族為研究目標者，不能僅依被研究者之同意，並應諮詢、取得該「原住民族」之同意方可進行之。

  而雇主招募或雇用員工時，除應遵守個資法規範，亦應注意不可違反求職人或員工之意思，要求其提供非屬就業所需之隱私資料，於此無論是否有經當事人書面同意，皆有違反相關法規之虞。如某派遣公司應徵電話客服員，卻要求錄取之員工需提供梅毒血清檢驗項目結果等體檢報告，便因違反就業服務法遭開罰 3 萬元。
- 特種個資之利用：過往如欲向其他組織調閱資料，常會遭受以基於個資法保護的目的，不予提供個資檔案，尤其特種個資更是如此，但為了協助公務機關執行法定職務或非公務機關履行法定義務之情形下，得例外提供特種個資。因此如醫院接獲警調來函要求調閱資料，則應保留相關函文，並經院內審核流程後，以適當之方式提供予個資需求單位，並保存相關紀錄，以有效降低個資風險，並促進個資之合理利用。

2. 參考資料：
   - 提供健康檢查義務：職業安全衛生法第 20 條。
   - 特種個資：個資法第 6 條、施行細則第 4 條。
   - 原住民研究：人體研究法第 15 條。
   - 英國-敏感個資：Data Protection Act 1998, Part I Preliminary 2. Sensitive personal data。
   - 歐盟-GDPR 敏感個資：GDPR Article 9。
   - 就業服務法第 5 條第 2 項第 2 款。
   - 就業服務法優先適用於個資法：法務部 102 年 12 月 05 日法律決字第 10200683900 號函釋。

五、【行銷活動】某電信業者 D 是否可向消費者發送行銷訊息，或組織出版刊物？

1. 說明：

許多組織蒐集個資，多是希望透過發送訊息或通知，行銷其服務或產品，而個資法針對組織於行銷時亦有諸多限制，甚至目前已經有組織因為違反個資法關於行銷之規範，而遭到行政罰鍰的處分，故更應注意：

- 一旦當事人表示拒絕接受行銷，組織應即停止利用其個人資料行銷，並確保該筆個資後續不會再被其他部門誤用，而再次對其行銷。
- 組織於首次行銷時，應提供當事人拒絕接受行銷之方式，並支付所需費用，如免付費客服電話，或以電子郵件寄送行銷訊息時，提供連結讓當事人可選擇拒絕接受訊息。
- 除此之外更應注意者，如果組織所蒐集之個資係屬違法取得，本應依個資法規定主動刪除、停止蒐集、處理或利用該個人資料，而不能主張當事人並未行使拒絕行銷之權利而利用該資料。

2. 參考資料：

- 行銷規範：個資法第 20 條第 2、3 項。
- 違法取得個資：個資法第 11 條第 4 項。

六、【社群軟體】某傳播業者 E 透過社群軟體或粉絲團舉辦活動蒐集個資時，該注意哪些重點？

1. 說明：

許多組織會透過方便的社群軟體，如 FB、LINE、部落格等媒介舉辦活動，希望能推廣其產品或服務，但於此同時，亦有可能透過蒐集個資的過程，將資料與社群軟體以外的個資做整合，都將可能會對個資當事人造成很大的影響，所以組織如欲透過社群軟體等媒介蒐集個資，應注意以下重點：

- 透過會員招募、抽獎、比賽或投票等各種行為蒐集個資時，應向當事人踐行告知義務。
- 應提供當事人行使當事人權利的管道，以保障其權益，如於活動頁面上提供客服專線或客服信箱等。
- 需留意保存於 FB 或 LINE 上含有個人資料的聯絡訊息，是否亦同樣納入組織個人資料保護與管理之範疇中，如是否將其納入盤點範圍，並設定保存期限，以及定期清查刪除檔案等作為。
- 如活動係委託行銷策劃公司等代為蒐集、處理或利用個資時，應善盡對受託公司之監督與管理（詳參閱第八問）。

2. 參考資料：

- 告知：個資法第 8 條。
- 當事人權利行使：個資法第 3 條。
- 拒絕行銷：個資法第 20 條第 2、3 項。

- 委外監督管理：個資法第 4 條、施行細則第 8 條。

七、【客戶服務】消費者乙要求某電信業者 F 刪除其個人資料，F 該如何處理？

1. 說明：

個資法賦予個資當事人查詢、閱覽、請求製給複製本，並得要求停止蒐集、處理或利用，以及刪除其個資的權利，因此當組織接收到消費者提出欲刪除其個資之要求，可參考以下方式執行之：

- 確認當事人人別：組織應先行確認行使當事人權利者，係本人或有權代理本人之人，如備有委託書、證件，或可證明為父、母、監護人等，方可確保此申請確實為本人或可代表本人所提出。
- 申請審核：針對當事人所提出刪除其個資之申請進行審核，確認是否符合以下情形，作為准駁當事人聲請與否的依據：
  - 當初蒐集個資之特定目的仍然存在。
  - 個資檔案保存期限尚未屆滿。
  - 因執行職務或業務所必須，尚不能刪除或停止蒐集、處理或利用個資（如雇主應置備勞工名卡，登記勞工之相關個資，並保管制勞工離職後 5 年，故如有離職 2 年之員工提出刪除其個資之請求，得依法暫時拒絕之）。
  - 經當事人書面同意，尚不能刪除或停止蒐集、處理或利用個資。
- 作業時程：依個資法規範，刪除或停止蒐集、處理或利用之申請處理，應於 30 日內為准駁之決定，必要時得延長，但不得超過 30 日，並應將其原因已書面通知當事人。
- 申訴或諮詢窗口：為確保個資當事人能有明確行使其權利之管道，組織應應設置申訴或諮詢窗口，且該行使權利之方式及管道，應明確並便利當事人使用，不宜以不適宜的方式妨礙其行使之，如：要求當事人必須親自至某公司位於阿里山山頂辦事處臨櫃申請，才能行使當事人權利。

2. 參考資料：

- 當事人得行使權利：個資法第 3 條
- 刪除、停止處理或利用：第 11 條第 3、4 項。
- 備置勞工名卡：勞動基準法第 7 條。
- 作業時程：個資法第 13 條。

八、【業務委外】某電視購物業者 G 將快遞業務委由物流業者 H 執行，G 該如何善盡監督責任？

1. 說明：

組織礙於現實成本、資源之考量，會將部分業務委託給外部廠商代為執行，倘所委託之業務涉及個人資料之蒐集、處理或利用時，則委託方（組織）亦應對受託方（外部廠商）違反個資法規定之行為負法律責任，因此委託方得參考以下重點，作為監督受託方的作為：

- 廠商遴選：組織於辦理委託業務，擇選廠商時，可以要求廠商說明其對於個資保護之要求與作為，甚至是否有通過個資管理制度（如 TPIPAS）驗證，或可提供個資保護自我評量表，作為瞭解廠商內部對於個資保護的能力。
- 合約簽署：組織如能於合約中，明訂雙方應遵守之行為規範，將可明確雙方的權利義務，以及能落實對於個資安全的保護，以及後續的責任歸屬。
- 定期監督：相較於合約簽署等作為，組織如能實際對受託廠商進行監督查核，積極落實管理機制，亦能更有效要求廠商遵守合約所約定內容。
- 定期評鑑：針對受託廠商今年度執行業務，以及辦理個資保護與管理制度措施進行綜合評鑑，以瞭解廠商是否確實能完整妥善執行受託業務，並作為來年續約或合作條件商議的參考標準之一。

另外亦需注意者，組織於委託受託廠商的業務流程中，如有特別需要約定的事項，亦可依照施行細則第 8 條第 2 項第 5 款的規定，約定保留指示之事項，如：

- 受託廠商如受組織委託蒐集個資，應代為履行告知義務；
- 受託廠商如受組織委託處理個資，其執行的方式及應遵循的程序要求；
- 受託廠商如受組織委託利用個資，其利用的方式及應遵循的程序要求；
- 受託廠商如接到當事人依照個資法第 3 條行使其權利，應由受託廠商或組織來處理，以及該如何處理等程序細節。

2. 參考資料：
   - 委託：個資法第 4 條。
   - 監督受託廠商：個資法施行細則第 8 條。

九、【國際傳輸】某電信業者 H 可否將含有個人資料的檔案傳送至國外的部門、分公司或是合作飯店？

1. 說明：

在現今網際網路蓬勃發展，各種新型態的資料傳輸、儲存及運用方式誕生，使個資更順暢於國際間流通，而使個資於國際間傳輸的資料保護更顯重要，而與部分國家採取原則禁止，例外開放的情形不同，我國乃採取原則開放國際傳輸，例外由中央目的事業主管機關限制的規範，因此組織於進行個資檔案國際傳輸時應注意以下幾點：

- 是否有違反個資法規範，而遭到中央目的事業主管機關限制之業務，如我國目前僅有限制通訊傳播事業經營者將所屬用戶個資傳遞至大陸地區。
- 是否有違反國際個資傳輸規範，而有可能將資料國際傳輸時，違反其他國家或組織之規定，如歐盟通用資料保護規則（General Data Protection Regulation, GDPR），或 APEC 隱私保護綱領（APEC Privacy Framework）中所提及之跨境隱私保護規則(Cross Border Privacy Rules, CPBR)等。

2. 參考資料：

- 國際傳輸：個資法第 21 條。
- 國際傳輸限制：遠通傳訊字第 10141050780 號。

十、【資訊安全】組織如果想加強其資料保護，該如何落實資訊安全防護？

1. 說明：

組織目前多仰賴資訊技術設備來管理所保存之個資檔案，而資訊安全亦為個資保護所重點關注的一環，甚至有部分組織個資外洩，皆肇因於資訊安全防護的不足，因此建議組織於落實資訊安全防護時，可參考以下重點：

- 作業面管控措施：

  組織應建置資訊安全管理程序，設立資訊安全標準以供人員遵守，而程序內規範如下，組織可視需求採行之：

  - 清查組織內使用之系統，明確設置管理權限並定期查核之。
  - 裝設防毒軟體及防火牆，減少駭客入侵機會。
  - 設置業務終止後檔案及設備處理辦法，避免已刪除之檔案或報廢之硬碟被還原而遭到不當利用。
  - 規範密碼管理、保存及應用管理，要求密碼強度設定，並定期更換密碼，降低因密碼管理不當或過於簡單而被破解的風險。
  - 規制資料備份機制，完善資料備份，妥善評估紙本或電子檔案保存之安全性，並定期檢視備份之完整性，以防資料遭到毀損無法恢復之風險。
  - 要求軟體定期進行更新，並避免使用無法更新、停止更新，或非法、無授權之軟體。
  - 於系統開發測試時，使用匿名化或虛擬之個資，以及檢視程式原始碼資料等工作。
  - 將保有重要個資檔案之磁碟予以區隔，以內網限制其連外之情形。
  - 定期對員工進行教育訓練，並針對權責不同人員予以進階教育訓練，加強其專門資訊安全控管能力。
  - 設置事故應變處理機制，並定期演練檢討，以強化員工面對事故處理之反應能力。

- 技術面管控措施：

  組織可於業務操作過程中加設管控措施，以技術控制減少個資外洩風險：

  - 對於紙本傳遞或電子檔案傳輸加強管控措施，如紙本彌封公文袋，或檔案傳輸加密功能等。
  - 限制員工遠端連線存取公司內部系統之情形。
  - 加強系統異常監測作業。

- 物理性控管措施：

  - 設置進出入門禁管制，落實檢查與紀錄機制，避免無權限人員任意進入保存重要個資

檔案之場所。

- 確保監視錄影設備正常運作，如確實保留紀錄、定期時差調校等。

2. 參考資料：

- 資訊安全要求：個資法施行細則第 12 條第 2 項第 6、第 8 款。

十一、 【人員管理】某電信業者 V 該如何降低員工因故意或過失而引起之個資外洩事故？

1. 說明：個資發生外洩有時係因為組織對於內部人員之管理不當所造成，因此組織如欲加強對人員管理之要求，可從管理面、法律面及技術面著手：

- 加強員工教育訓練：培養其基本個資保護概念，並使其瞭解並能確實落實組織個資保護與管理政策與各項程序、辦法。
- 落實審核機制：確保組織於蒐集、處理或利用之流程，接能透過適當之審核機制，避免無授權之濫用行為發生。
- 與員工簽訂保密協議：明訂員工於個資保護上之權利義務，並透過保密協議提醒員工如違反法令之風險及後果。
- 建置管控設備：於員工操作之系統上安裝防護軟體，如防毒軟體、加密軟體等，減少個資外洩可能性。

而組織為有效執行事故應變管理措施，可採行以下方式：

- 評估組織資源與人力，擬定事故應變計畫，以便在事故發生當下能快速因應，減少並控制損害的範圍。
- 於查明事故之狀況後，以適當方式通知當事人，通知內容應包括外洩的事實、組織所採取之措施，以及提供諮詢服務之管道。
- 如係屬重大個資事故，應即通報通傳會（所謂重大個資事故，係指個人資料遭竊取、竄改、毀損、滅失或洩漏，將危及非公務機關或大量當事人權益之情形）。
- 透過常時的事故應變演練，或事故處理後之檢討改善，以確保相關人員皆能瞭解其於事故發生時應扮演之角色及職責，並進而精進組織內個資保護管理制度措施，以降低個資保護與管理風險。

2. 參考資料：

- 事故之預防、通報及應變機制：個資法施行細則第 12 條第 2 項第 4 款。

十二、 【APP 開發】某電信業者 K 於開發 APP 供消費者使用時，該注意哪些重點？

（最小蒐集原則、APP 分級）

1. 說明：

行動應用程式（Mobile Application，簡稱 Mobile app、apps）現在儼然成為組織於推展業務時的重要工具，而其更能快速便捷地大量蒐集個資，因此組織透過 APP 向用戶蒐集個資時，應注意以下

內容：

- 最小必要性蒐集原則：組織應衡酌使用該 APP 所需蒐集之必要個資，以避免過度蒐集個資，減少個資控管風險。
- 告知或隱私權政策：組織應於蒐集當事人個資的當下，告知其依個資法應告知之內容，俾便當事人瞭解其個資於組織中使用的情形，作為衡量是否提供個資的依據。

  或，組織可透過隱私權政策，告知當事人你的 APP 蒐集的個資欄位、目的，個資將會儲存於何處，以及會基於何種理由與哪些人共享這些資訊，其他尚有如資料保存的期限，以及當事人權利行使的管道。
- 原始碼檢測：如組織係委託 APP 開發商或第三方服務（如分析或廣告網站），則由於這些受託廠商也有可能會蒐集到當事人個資，因此組織亦應明確瞭解受託廠商執行業務時的確切情況，並予以監督控管，以降低個資風險。
- 是否提供途徑以供用戶拒絕：組織因蒐集了當事人的個資，基於保障當事人個資自決權，以及符合個資法規範，當然應提供其行使權利之管道，並確實依照當事人之聲請執行之。

2. 參考資料：
   - 最小必要性蒐集原則：個資法第 5 條。
   - 告知：個資法第 8 條。
   - 當事人權利行使：個資法第 3 條。

十三、 【稽核改善】組織該如何確保所建置之管理制度係正常運作且能持續改善？

1. 說明：

   組織於建置個人資料保護與管理制度後，為確保組織內部能有效遵照相關程序之要求，通常會定期（每年至少一次）進行檢視，而檢視亦可分為組織內部人員執行之內部稽核（又稱內部評量），或由外部公正第三方執行之外部稽核，而有效之稽核工作應至少保含以下內容：

   - 稽核計畫：組織可視規模、成本，規劃全組織、全範圍，或是具高風險業務之部門、流程優先受檢。
   - 稽核報告：稽核過程應由具備相關專業證照或經驗之人員主導，並於查核完成後出具正式的稽核報告，並交由最高管理階層審核之。
   - 追蹤改善：組織應審閱稽核報告中之待改善事項，審慎評估應改善之措施，並追蹤改善之情形，以確保缺失已改善。

   除稽核報告之外，組織也應衡酌法規修改狀況、主管機關函令、利害關係人的要求、以及組織內外部之改善建議，以及社會情勢、國民認知、技術發展等各種環境的變遷，定期調整與修正個人資料保護與管理制度，以期得與時俱進，並能符合實際需求。

2. 參考資料
   - 資料安全稽核機制：個資法施行細則第 12 條第 2 項第 9 款。

- 個人資料安全維護之整體持續改善：個資法施行細則第 12 條第 2 項第 11 款。

參、 支援協助篇

一、【法令遵循】某法務人員丙想瞭解公司於個資法之法遵需求，丙該搜尋哪些與個人資料保護有關的法令規範？

1. 說明：

組織除了應遵守個資法及個資法施行細則之規範外，尚有其他與個人資料及隱私保護相關的法規尚待遵從，故組織應定期盤點檢視作業流程相關之法規，並評核目前執行業務之方式是否與法規相符，如有違法之虞者便可予以修改，而組織可參酌之其他法令規範有：

- 依循個資法由各目的事業主管機關公布施行之子法：目前各目的事業主管機關以逐步針對轄下主管事業，推出安全維護辦法及業務終止後處理辦法，俾便各事業可依其產業之特性，落實個資保護管理。如國家通訊傳播委員會（NCC）訂定「國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法」、內政部訂定之「當鋪業個人資料檔案安全維護管理辦法」或經濟部訂定之「網際網路零售業及網際網路零售服務平台業者個人資料檔案安全維護辦法及業務終止後處理作業辦法」等。
- 其他特別法：如銀行法要求銀行對於客戶之存款、放款或匯款等相關資料，應保守秘密，又或醫院及醫師等相關醫事人員，不得無故洩漏病人之病情或健康資訊，等依行業或事務特別性而立之專法。

2. 參考資料：

- 子法：個資法第 27 條第 2、第 3 項。
- 銀行對於客戶資料之保密：銀行法第 48 條第 2 項。
- 醫院及醫事人員之保密：醫療法第 73 條。

二、【輔導資源】某新創公司 L 如果希望導入個人資料保護與管理制度，但礙於人力與專業不足，可向誰尋求協助？

1. 說明：

對於組織而言，如要完整且確實的推動個人資料保護與管理制度，往往礙於人力與專業的限制，而遭遇到推動的困難，因此如果組織有導入制度的意願，但苦於缺乏導入的經驗與專業知識，皆可透過以下管道尋求協助：

- 國家通訊傳播委員會為提供通傳業者個人資料保護與管理必要資源，特委請資策會科法所協助通傳會官網【隱私保護機制專區】，提供個資保護與管理法遵文件與常見問答集等相關資料，希冀業者能藉此完善當事人個資及隱私保護，並強化組織內部管理健全。

  國家通訊傳播委員會【隱私保護機制專區】網址連結：

  https://www.ncc.gov.tw/chinese/news.aspx?site_content_sn=5011&is_history=0
- 除此之外，業者亦可參考本文件「肆、 結語：因應個人資料保護與管理之實務作法」之內容，選擇適當之管理制度以協助建置組織內部個資保護與管理制度。

肆、 結語：因應個人資料保護與管理之實務作法

目前國內相關採行的相關管理實務標準制度如下：

一、 臺灣個人資料保護與管理制度（Taiwan Personal Information Protection and Administration System, TPIPAS）：

1. 背景沿革

行政院於 2009 年 8 月「塑造資安文化、推升資安產值」產業科技策略會議中，決議推動電子商務個人資料管理暨資訊安全行動方案，並於 2009 年 12 月核定關鍵推動方案，其中之一，即是希望透過政府與民間組織之合作，達到「強化民眾個資保護」目標，以解決資料不當利用造成之個資外洩或隱私侵害問題。

然國內組織在面對個資法繁複之規定，對於內部個人資料如何管理以符合法遵需要，有如何適用之需求，因此，為提供各產業有一法規遵循機制，協助組織內部進行個人資料管理工作，提升國內個資保護水準，活絡商務交易活動，即依循我國個資法，輔以管理流程 P（Plan）-D（Do）-C（Check）-A(Action)概念，並參酌如韓國、日本、德國等主要國家推動經驗，由經濟部商業司委託財團法人資訊工業策進會科技法律研究所建置及推動完善我國個人資料管理制度 TPIPAS，其不僅係唯一一部以我國個資法為基石協助產業達到法遵要求之個資管理制度，亦可與國際管理制度及隱私權相關規定接軌，符合國際趨勢，有助組織跨國貿易之進行與展開。

雖然本方案之初衷，係在於協助國內電商產業建立個資保護管理制度，但時至今日，TPIPAS 以可供不論是公務或非公務機關，抑或是否為經濟部商業司轄下主管事業，皆可導入本制度，以期全面提升臺灣個人資料保護與管理水平。

於此同時，為了強化輔導工作能量，並積極擴展及協助本制度導入，TPIPAS 亦與業界輔導機構合作，希望透過輔導機構一同推動本制度，以協助有意願導入之組織能更完善建置 TPIPAS。

因此，TPIPAS 不僅可作為組織遵循個人資料保護法具體作為之準繩，更可透過管理制度 P-D-C-A 的循環，持續精進組織內部管理制度，使組織體質強化，而於導入同時，亦可透過 TPIPAS 提供之協助與支援，使能更有效率完成制度建置。

2. TPIPAS 驗證取得資料隱私標章標章（Data Privacy Protection Mark, dp.mark），或特定範圍檢視取得證書

對於自行導入 TPIPAS 或是經由輔導顧問機構協助導入 TPIPAS 的組織，如果覺得制度文件已經完善，組織內部對於制度之推展業已成熟，便可評估是否要向 TPIPAS 制度維運小組提出驗證或特定範圍檢視的申請，並可預期將帶來以下效益：

◆ 降低組織法律風險：

當組織因個資事故造成當事人之損失，除能證明事故發生係非故意或過失，才能免除損害賠償責任，而如能導入管理制度，組織於辦理個資業務時，不僅可受到必要的規範，以減少事故發生可能，亦能於發生事故時快速因應處理，降低損害範圍，更能規律有效低保留必要管理審核紀錄，作為後續法庭上舉證的證據。

- 對於個人而言：

  員工可以透過對管理制度的瞭解，明確遵守個資法相關規範，以避免以身試法，而組織負責人、代表人或其他有代表權之人，亦可憑藉對制度的支持與推動，證明其對於組織個資保護的監督與作為，以免遭受到與組織同一額度罰鍰之處分。

- 提升組織管理能量：

  管理制度不僅可以協助降低組織法律風險，更可以透過持續 P-D-C-A 循環，改善組織內部作業流程，將個資保護意識深植並內化於員工心中及日常業務的作為，使生活處處有個資，作業時時有防護，如此亦可提升組織能量，強化後續各種專案推動的效率與效能。

- 透過標章、證書，提升組織形象：

  組織欲取得管理制度標章（如 dp.mark）或證書，皆須透過公平、公正、公開的驗證機制，因此對於持有標章與證書的組織而言，皆表彰組織對於個資隱私保護的重視，藉此不僅可提升組織形象，更可加強消費者將個資交給組織的意願及信賴感，是故對於組織而言，導入個資保護與管理制度，確實為組織於營運上值得參考的投資。

二、 ISO 國際標準

ISO 自 2011 年發展出 ISO 29100 隱私權框架後，已陸續發展出 ISO 29191 部分匿名及部分去連結鑑別之要求事項、ISO 29101 隱私權架構框架（Privacy architecture framework），並於 2017 年發展出適用於一般組織的隱私衝擊評鑑的國際標準「ISO 29134：隱私衝擊評鑑指引」，以及個資保護控制措施的國際標準「ISO 29151：個人可識別資訊保護實務」

而對於已經通過 ISO27001 資訊安全管理系統驗證的組織，於驗證時，ISO 則建議以延伸 ISO27001 的方式實施，依照組織實際需求的差異，以補強原先驗證深度與廣度的不足。如 ISO27001：2013 標準附錄 A 中所列各項控制目標及控制措施中並未完善對個人資料保護之要求，故於制度導入以至驗證時，可加入 ISO29151 以識別個人資料風險及其對應個人資料保護的控制措施。

三、 BS10012 英國個人資訊管理系統（Personal Information Management System；PIMS）

1. 背景沿革

為保障英國國人個人資料保護與管理，英國在 1998 年制訂了資料保護法案（Data Protection Act 1998），並且在 2000 年公布實施，要求資料保護者需遵守法律的規範及要求，以保護個人資料的蒐集、處理及利用的過程。而英國標準協會，遂於 2009 年 5 月 31 日公布個人資訊管理系統（Personal Information Management System；PIMS）標準，供組織建置制度。

而為因應歐盟於 2016 年 4 月通過，並於 2018 年 5 月 25 日正式實施的「通用資料保護規章（GDPR）」新版 BS10012：2017 已經於 2017 年 3 月 31 日正式發布，期盼能使依循本制度的組織，接能符合歐盟 GDPR 的規範，並降低組織法律上的風險。

2. 制度維運

對於欲導入 BS10012 的組織而言，可以參考的步驟如下：

- 開始：透過對於 BS10012 制度的理解，瞭解制度能產生之效益以及相關制度建置計畫的執

行內容。

- 建 置 ： 依照組織欲保護個人資料之重要性以及組織可負擔之成本，建置符合組織需求之個人資料保護與管理制度。
- 驗 證 ： 透過對組織所建置管理制度的驗證工作，確保組織內流程和控制措施的建置狀況，係符合 BS10012 之規範要求。
- 維 護 ： 確保企業所建置的管理制度持續改善，以維持個資保護與管理的最佳效益。