

這樣做就對了！

中小企業對客戶的個人資料保護手冊



個人資料保護委員會籌備處 —— 編著
Preparatory Office of the Personal Data Protection Commission

目錄

前言

第1章 什麼是個人資料？ 3
個人資料的基本概念

- 什麼是個人資料？ 4
- 企業常接觸的個人資料包含哪些？ 5

第2章 誰要蒐集個人資料？ 6
個人資料的蒐集主體

- 誰是個人資料的蒐集主體？ 7

第3章 哪些個人資料與業務如影隨形？ 8
個人資料的蒐集

- 蒐集個人資料時該注意什麼？ 9
- 蒐集個人資料時該告知什麼？ 13

第4章 因業務而保有個人資料該注意什麼？ 15
個人資料的管理

- 中小企業容易達成的「適當安全維護措施」 16
- 需刪除個人資料的情形與正確做法 17
- 個人資料外洩時該怎麼做？ 18

第5章 於蒐集目的外利用個人資料時該注意什麼？ 19
個人資料與第三方

- 於蒐集目的外利用個人資料時該注意什麼？ 20

第6章 當個人資料當事人權利行使時該怎麼辦？ 21

- 個人資料當事人權利行使時如何回應？ 22

附　錄 各目的事業主管機關個人資料檔案安全維護辦法 24



前　言

為了協助屬於個人資料保護法所稱「非公務機關」的中小企業主快速瞭解如何落實個人資料保護的正確做法，本書將深入淺出介紹中小企業在落實個人資料保護時需要留意的事項，以及重要的個人資料保護基礎概念。

期待能藉由本手冊，協助中小企業主提升個人資料保護意識，建立個人資料保護正確觀念，並在商業活動中強化對顧客個人資料保護的透明度、安全度以及誠信，遵循個人資料運用的比例原則，以進一步獲得顧客的信任，使企業主與顧客獲得雙贏。

個人資料保護法

個人資料保護法施行細則





第1章

什麼是個人資料？

個人資料的基本概念

什麼是個人資料？ 4

企業常接觸的個人資料包含哪些? 5

什麼是個人資料？

只要是與目前活著的某個自然人有關，且能據此識別出是那個特定人的資料，就是個人資料。



常見的個人資料類型包含

01 可以直接識別出某人的資料



透過資料本身，就可以直接連結到某一個特定的人。

例如：姓名、身分證號碼、照片、指紋等。

02 可以和其他資訊結合，間接識別出某人的資料



除了資料本身以外，還需要將資料跟其他的資訊互相對照、組合或連結。才能識別出某一個特定的人。

例如：地址、電話、車牌號碼、照片、出生年月日、特徵、職業、婚姻、財務狀況等。

個人資料保護法保護的個人資料是否以生存的人為限？

個人資料保護法的立法目的之一，就是保護人格權中的資料隱私權，因此只有目前生存的自然人，才會有隱私權受到侵害的恐懼情緒，故已死亡的人的個資不受個人資料保護法的保護。

· 參考規範 ·

- 名詞解釋：個人資料保護法第2條第1款
- 個人定義：個人資料保護法施行細則第2條

企業常接觸的個人資料包含哪些？

通常企業會接觸到的個人資料，以「顧客」的個人資料為大宗，例如顧客消費時提供的聯絡方式、消費紀錄，都屬於個人資料的一環。



企業經常接觸的個人資料
以顧客消費行為相關的個資為主



顧客消費時的個人資料



Line、APP會員註冊

- 姓名
- 出生年月日
- 電子信箱
- 手機號碼

等相關資料。



消費時

- 消費紀錄
- 信用卡號碼
- 宅配地址
- 住家電話

等相關資料。



其他企業與顧客間的互動

- 客服對話
- 問卷調查
- 社群互動
- 瀏覽紀錄

等相關資料。

重點說明

如果蒐集到的個資是特種個資，包含病歷、醫療、基因、性生活、健康檢查及犯罪前科等，原則不能蒐集、處理或利用，但如果例外符合個人資料保護法規定的情形（如：取得當事人的書面同意），就可以合法運用。

· 參考規範 ·

| 特種個資：個人資料保護法第6條



第2章

誰要蒐集個人資料？

個人資料的蒐集主體

誰是個人資料的蒐集主體？

不論是自然人、法人或其他團體，只要向當事人蒐集個人資料，就會成為個人資料的蒐集主體。



中小企業本身就是個人資料保護法的蒐集主體

中小企業

蒐集主體

- 可以掌握個資，決定個資處理目的或方法。
- 中小企業以自身的名義向顧客蒐集個人資料時，就是個人資料的蒐集主體。

內部構成員

內部員工

- 依照蒐集主體的內部指示，進行蒐集、處理或利用個人資料。
- 例如：餐廳員工受老闆指示，蒐集顧客的姓名及聯絡方式。

外部委託及監督責任

外部受託者

受託處理者

- 受蒐集主體的委託，為其蒐集、處理或利用個人資料。
- 例如：餐飲業者將客戶資料管理業務委託給資訊服務公司處理。

·參考規範·

非公務機關定義：個人資料保護法第2條第8款

受託者視同委託機關：個人資料保護法第4條
個人資料保護法施行細則第7條、第8條



第3章

哪些個人資料與業務如影隨形？

個人資料的蒐集

蒐集個人資料時該注意什麼？ —— 9

蒐集個人資料時該告知什麼？ —— 13

蒐集個人資料時該注意什麼？

在蒐集個資時，中小企業應該要有明確的特定目的（業務上用途），符合法定的要件，並且蒐集個資的範圍必須與目的有正當合理的關聯，符合比例原則。





· 參考規範 ·

- 符合特定目的、比例原則：個人資料保護法第5條
- 非公務機關蒐集或處理個資要件：個人資料保護法第19條第1項

蒐集個人資料時該注意什麼？

情狀一：顧客線上下單購買紙本禮券



符合法定要件

顧客線上購買禮券，與線上商城建立買賣契約。線上商城處理時蒐集顧客的個資合理且必要，無需另行取得顧客同意。

蒐集要符合（業務上的）特定目的

線上商城因「**顧客線上下單購買禮券寄送**」的目的，需要取得顧客的個人資料。

僅蒐集必要範圍

因「**顧客線上下單購買禮券寄送**」的目的，線上商城只要蒐集顧客與物流相關的姓名、地址及聯絡方式，就能夠提供前述服務，因此蒐集與目的間具有正當合理的關聯，且只蒐集了必要的個資。

合規蒐集的個資



不符合特定目的之案例

例如：某健身房舉辦免費健康講座，除了參與者的姓名，也蒐集了參與者的信用卡資料，然而免費活動應不需要蒐集到信用卡相關資料，此即不符合特定目的。



· 參考規範 ·

- 非公務機關蒐集或處理個資要件：個人資料保護法第19條第1項
- 契約或類似契約之關係：個人資料保護法施行細則第27條

蒐集個人資料時該注意什麼？

情狀二：為通知手機到貨留下聯絡方式





蒐集要符合（業務上的）特定目的

商家因「通知手機到貨」的目的，需要取得顧客的個人資料，包含姓名、聯絡方式。

符合法定要件

契約成立前，買賣雙方為了商議訂定契約，交換個人聯絡方式，即符合蒐集的法定要件。

僅蒐集必要範圍

因「通知手機到貨」的目的，商家只要蒐集顧客的姓名、聯絡方式，就能夠提供前述服務，因此蒐集與目的間具有正當合理的關聯，且只蒐集了必要的個資。

合規蒐集的個資



· 參考規範 ·

- 非公務機關蒐集或處理個資要件：個人資料保護法第19條第1項
- 契約或類似契約之關係：個人資料保護法施行細則第27條

蒐集個人資料時該注意什麼？

情狀三：顧客用餐後參加意見回饋活動



蒐集要符合（業務上的）特定目的

商家基於「**提供優惠訊息**」的目的，需要取得顧客的個人資料。

符合法定要件

顧客在用餐後主動填寫滿意度調查表中的個資欄位，或是同意提供個資，均符合蒐集的法定要件。

僅蒐集必要範圍

因「**提供優惠訊息**」的目的，只要蒐集顧客的姓名、聯絡方式，就能夠提供前述服務，因此蒐集與目的間具有正當合理的關聯，且只蒐集了必要的個資。

合規蒐集的個資



· 參考規範 ·

非公務機關蒐集或處理個資要件：個人資料保護法第19條第1項

蒐集個人資料時該告知什麼？

為了讓當事人更清楚了解個資將如何被使用，企業在蒐集當事人的個資時，原則應向當事人告知以下的法定事項。



如是當事人提供個資（直接蒐集）時，企業應告知：

01 名稱

例如：
○○股份有限公司。

02 蒐集目的

例如：
為了客戶管理與提供服務。

03 將蒐集哪些類型的個人資料

例如：
姓名、電子信箱、手機號碼。

04 預計如何利用個人資料

包含：
利用的期間、地區、誰會利用、如何利用。

05 顧客可以行使哪些權利

例如：
要求查詢、提供複製本、更正、刪除等。

06 如果顧客未提供個資會影響哪些權益

例如：
顧客可選填地址，如未填寫則無法提供宅配服務。

如不是當事人提供（間接蒐集）時，企業應告知：

其蒐集個資的來源 ＋ **前述01~05所列事項**

企業告知法定事項的方式

企業可以透過言詞、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進行告知。

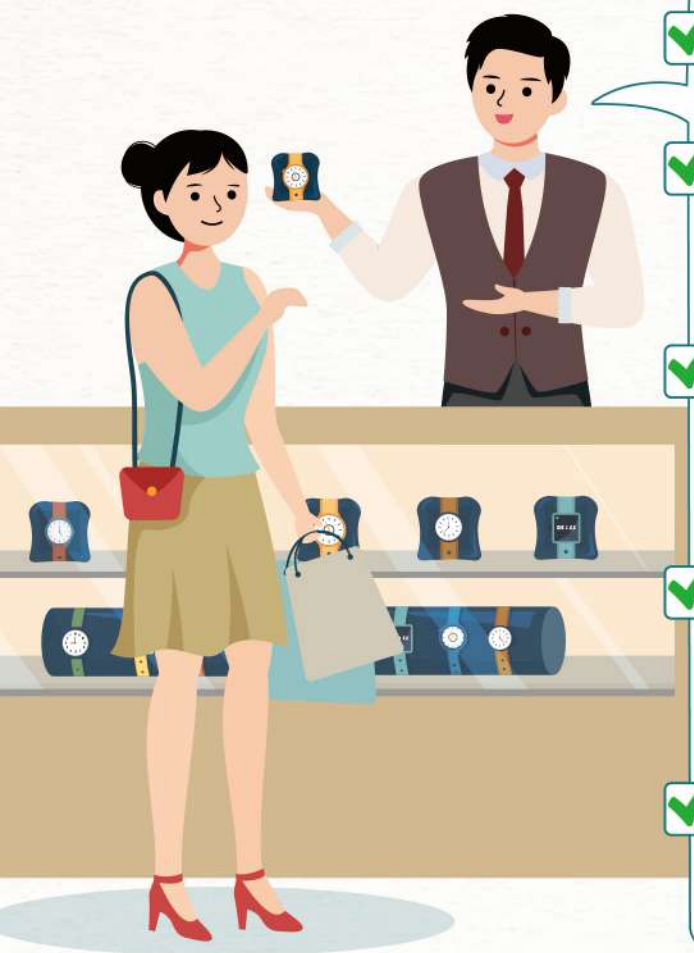
· 參考規範 ·

- 蒐集當事人提供個資時應告知事項：個人資料保護法第8條第1項
- 蒐集非當事人提供個資應告知事項：個人資料保護法第9條第1項
- 向當事人告知方式：個人資料保護法施行細則第16條

蒐集個人資料時該告知什麼？

對當事人進行告知的實際範例

例如：消費者向鐘錶店預約新款手錶



- 您好：我們是OO鐘錶公司。
- 為了提供您預定手錶的服務，本公司將請您提供您的姓名、手機號碼以利通知取貨。
- 在您預定的商品到貨之時，本公司將利用您先前留下的個資，通知您商品到貨，本公司並將在您取貨後依法刪除保有的個資。
- 您可以向本公司主張個人資料保護法上的相關權利：要求查詢您在本公司保存的個資、提供個資複製本、更正、刪除您在本公司保存的個資。
- 如您另外提供地址資訊，本公司可再提供宅配服務。

·參考規範·

蒐集當事人提供個資時應告知事項：個人資料保護法第8條第1項



第4章

因業務而保有個人資料該注意什麼？

個人資料的管理

中小企業容易達成的「適當安全維護措施」 16

需刪除個人資料的情形與正確做法 17

個人資料外洩時該怎麼做？ 18

中小企業容易達成的「適當安全維護措施」

企業如保有個人資料檔案，應採行適當的安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。此外，也要維護保有個資的正確性。並於特定情形下，需刪除保有的個人資料。



中小企業容易達成的「適當安全維護措施」



內部員工
蓄意/意外洩漏風險

人員管理措施

- 制定並實施內部管理程序、配置管理人員。
- 人員管理：如人員權限管理、檢查員工異常資料流動、禁用非法軟體或公開雲端服務、避免危險上網行為、勿隨意開啟可疑郵件等。
- 教育訓練：如辦理個資安全教育訓練及演練等。



外部駭客
攻擊系統漏洞風險

技術措施

- 安全機制：如建立帳號驗證或存取機制及次數限制、建立身分驗證機制、資料假名化等。
- 定期維護：如購買正版防毒軟體、更新電腦系統或應用程式、進行弱點掃描、定期適當的備份、定期更新密碼等。



個人資料
未經授權攜出風險

物理控制措施

- 訂定辦公場所使用裝置或攜出規範。
- 設置物理防護：如警衛、門禁簽到管理、錄影監控、識別證刷卡、全程陪同訪客、嚴防尾隨事件、定期刪除個資等。
- 如廢棄或更換電腦，可將儲存資料的硬碟進行格式化。

· 參考規範 ·

- 非公務機關保有個資應採行適當安全措施：個人資料保護法第27條第1項
- 各類安全維護措施項目：個人資料保護法施行細則第12條

需刪除個人資料的情形與正確做法

個人資料的刪除

以下的情形，中小企業需要刪除保有的個人資料

蒐集個人資料的特定目的消失時

例如：商店街為辦理抽獎活動蒐集個資，獎項頒發後就應刪除。

個人資料保存期限屆滿時

例如：電商平台與顧客約定蒐集個資後將保存3個月，時限屆滿後就應刪除。

違反個人資料保護法時

例如：電商業者購買來路不明的個人資料，用於推播廣告進行行銷，該個人資料之蒐集未符合法定要件，違反個人資料保護法而應予刪除。



若業者A合規的蒐集個資，卻在無合法事由（例如：經當事人同意）情形下，將個資提供給業者B用於行銷，此提供行為因屬違法利用，將有相關法律責任。

此外，業者B的蒐集行為也屬於違法蒐集，亦有相關法律責任。業者B應立即刪除違法蒐集的個資，不得繼續保有及作任何後續利用。

正確的個人資料刪除做法

紙本文件

宜使用水銷等無法回復原狀的方式，將紙本個人資料文件銷毀。

個人資料檔案

留意是否已分別刪除電腦主機、雲端（包含資源回收桶）保存的檔案。

·參考規範·

- 「刪除」定義：個人資料保護法施行細則第6條第1項
- 應刪除個資之情形：個人資料保護法第11條
- 得不刪除個資的情形：個人資料保護法施行細則第21條

個人資料外洩時該怎麼做？

企業管理的個人資料，如有被竊取、洩漏、竄改或其他侵害的情形，企業應於查明後儘速通知當事人，以使當事人得以知悉個資遭違法侵害的情事，以及時採取補救措施或提起救濟。



個資外洩時查明後要儘速通知當事人



通知當事人

只要企業發現個人資料已被侵害的事實，不論是否確有違法責任，企業均應儘速通知當事人：

- 通知當事人的內容要包含：個人資料已被侵害的事實，以及已採取的因應措施。
- 適當的通知方式包含：言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他可以讓當事人明確得知訊息的管道均可。



視規定通報主管機關

依照各目的事業主管機關的規定：

- 通報有時間限制：通常要在72小時內通報主管機關。
- 要通報的內容可能包含：通報哪些機關、發生時間、種類、原因及摘要、損害狀況、個資侵害可能結果、擬採取的因應措施、擬通知當事人的時間及方式、是否於發現個資外洩後立即通報等。
- 宜以書面方式對主管機關進行通報。

· 參考規範 ·

- 個資受侵害時通知當事人義務：個人資料保護法第12條
  國家發展委員會109年8月3日發法字第1090017079號
- 通知方式之例示與例外規定：個人資料保護法施行細則第22條



第5章

於蒐集目的外利用個人資料時該注意什麼？

個人資料與第三方

於蒐集目的外利用個人資料時該注意什麼？

企業原則要在特定目的內利用個資

除有其他情形外，需經當事人同意，才可以在特定目的外利用個資

當事人同意目的外利用的實際範例

例如：電商業者將購物行為資料用於第三方廣告合作

- 您好：為了提供更貼近需求的廣告服務，希望徵詢您的同意，將您留存在本公司的購物數據提供給合作廣告商，讓他們能推送更符合您需求的廣告內容。
- 我們不會提供您的姓名、聯絡方式或付款資訊，只會將您的購物數據，例如購買或瀏覽的商品類型，提供給廣告商。
- 如果您選擇不同意，您的購物數據將不會被提供，您仍然可以使用本公司的服務。



企業如有意在特定目的外利用顧客個資，且沒有其他法定的特殊情形時，得採個資當事人同意方式為之。換言之，就需先明確告知顧客：除了原本特定目的以外的其他利用目的、範圍及同意與否對其權益的影響；再由顧客就前述事項單獨表示同意。

· 參考規範 ·

- 特定目的外利用情形：個人資料保護法第20條第1項
- 當事人同意之定義：個人資料保護法第7條第2項
- 單獨所為之意思表示：個人資料保護法施行細則第15條



第6章

當個人資料當事人權利行使時該怎麼辦？

個人資料當事人權利行使時如何回應？

個人資料保護法賦予個人決定是否揭露其個資、及在何種範圍內、於何時、以何種方式、向何人揭露，及對個資使用有知悉與控制權、更正權等權利。



NO.1 當事人有向企業請求答覆查詢、提供閱覽或製給複製本的個資知悉權



當事人的請求權，企業不可以要求預先拋棄或以特約限制。

答覆查詢

例如：顧客想查詢過去一年內在某餐廳的消費紀錄，確認自己的消費與積分累計情形，此時餐廳可以透過線上會員平台答覆查詢之結果。

提供閱覽

例如：顧客曾經參與旅館的住宿滿意度調查，想閱覽自己填寫的問卷調查內容，此時旅館可安排顧客到店內查看問卷填寫紀錄。

製給複製本

例如：顧客在零售商購物，需要過去1年的購物紀錄，故要求零售商提供購物紀錄複製本，零售商可透過郵寄或mail的方式提供購物紀錄的複製本。

在某些情形下，企業可以拒絕當事人的請求，例如妨害該蒐集機關或第三人之重大利益。

· 參考規範 ·

對當事人請求之回應：個人資料保護法第10條

個人資料當事人權利行使時如何回應？

NO.2 當事人有向企業請求維護個資正確性的個資控制權與更正權

為了維護個資正確性，企業應該：

- 主動或依當事人請求，更正或補充其保有的個資。
- 個資正確性有爭議時，主動或依當事人請求，停止處理或利用該個資。
- 蒐集個資的特定目的消失或期限屆滿時，主動或依當事人請求，刪除、停止處理或利用該個資。
- 違反個人資料保護法蒐集、處理或利用個資時，主動或依當事人請求，刪除、停止蒐集、處理或利用該個資。
- 因可歸責於企業的事由，沒有更正或補充個資，企業應在更正或補充後，通知曾提供利用的對象。



除當事人請求外，企業平時也有義務維護其保有的個資。

企業在一定期限內要書面回應是否同意請求

- 答覆查詢、提供閱覽或製給複製本：企業需在15日內決定是否同意，必要時得延長最多15日，並應將原因以書面通知請求人。
- 與維護個資正確性有關的請求：企業需在30日內決定是否同意，必要時得延長最多30日，並應將原因以書面通知請求人。



為了便利當事人行使個人資料保護法上的權利，企業宜建置處理當事人權利行使的相關程序。

· 參考規範 ·

- 個資正確性維護：個人資料保護法第11條
- 回覆當事人期限：個人資料保護法第13條



附錄

各目的事業主管機關個人資料檔案安全維護辦法

各目的事業主管機關個人資料檔案安全維護辦法

***各目的事業主管機關之個人資料檔案安全維護辦法全文，可參閱全國法規資料庫。

全國法規資料庫
https://law.moj.gov.tw/

序	主管機關	法規名稱
1	經濟部	電業與公用天然氣事業及加油站業個人資料檔案安全維護管理辦法
		製造業及技術服務業個人資料檔案安全維護管理辦法
		零售業個人資料檔案安全維護管理辦法
		自來水事業個人資料檔案安全維護計畫標準辦法
		著作權集體管理團體個人資料檔案安全維護管理辦法
2	財政部	報關業個人資料檔案安全維護管理辦法
		保稅倉庫及物流中心個人資料檔案安全維護管理辦法
		記帳士與記帳及報稅代理人個人資料檔案安全維護管理辦法
		菸酒事業個人資料檔案安全維護管理辦法
		公益彩券發行機構個人資料檔案安全維護管理辦法

各目的事業主管機關個人資料檔案安全維護辦法

***各目的事業主管機關之個人資料檔案安全維護辦法全文，可參閱全國法規資料庫。

全國法規資料庫
https://law.moj.gov.tw/

序	主管機關	法規名稱
3	交通部	汽車運輸業與計程車客運服務業個人資料檔案安全維護計畫及處理辦法
		民用航空事業個人資料檔案安全維護計畫及處理辦法
		船舶運送業個人資料檔案安全維護計畫及處理辦法
		交通部指定觀光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
		停車場經營業個人資料檔案安全維護計畫及處理辦法
4	數位發展部	數位經濟相關產業個人資料檔案安全維護管理辦法
5	文化部	電影事業個人資料檔案安全維護計畫及處理辦法
6	農業部	農藥販賣業個人資料檔案安全維護管理辦法
		農業金融業個人資料檔案安全維護管理辦法

各目的事業主管機關個人資料檔案安全維護辦法

***各目的事業主管機關之個人資料檔案安全維護辦法全文，可參閱全國法規資料庫。

全國法規資料庫
https://law.moj.gov.tw/

序	主管機關	法規名稱
7	衛生福利部	醫院個人資料檔案安全維護計畫實施辦法
		精神復健機構個人資料檔案安全維護計畫實施辦法
		私立長期照顧服務機構個人資料檔案安全維護計畫實施辦法
		護理機構個人資料檔案安全維護計畫實施辦法
		社會福利機構個人資料檔案安全維護計畫實施辦法
		中藥批發零售業個人資料檔案安全維護計畫實施辦法
		化粧品批發零售業個人資料檔案安全維護計畫實施辦法
		醫療器材批發零售業個人資料檔案安全維護計畫實施辦法
		西藥批發零售業個人資料檔案安全維護計畫實施辦法
		非輻射電子醫療器材設備製造業個人資料檔案安全維護計畫實施辦法
		食品業個人資料檔案安全維護計畫實施辦法
		社會福利財團法人個人資料檔案安全維護計畫實施辦法

各目的事業主管機關個人資料檔案安全維護辦法

***各目的事業主管機關之個人資料檔案安全維護辦法全文，可參閱全國法規資料庫。

全國法規資料庫
https://law.moj.gov.tw/

序	主管機關	法規名稱
8	內政部	內政部指定交友服務業個人資料檔案安全維護管理辦法
		內政部指定營建類非公務機關個人資料檔案安全維護管理辦法
		內政部指定政黨及全國性民政財團法人個人資料檔案安全維護管理辦法
		內政部指定祭祀團體個人資料檔案安全維護管理辦法
		內政部指定宗教團體個人資料檔案安全維護管理辦法
		內政部指定地政類非公務機關個人資料檔案安全維護管理辦法
		內政部指定合作及人民團體類非公務機關個人資料檔案安全維護管理辦法
		內政部指定殯葬服務業個人資料檔案安全維護管理辦法
		內政部指定移民業務機構個人資料檔案安全維護管理辦法
		內政部指定警政類非公務機關個人資料檔案安全維護管理辦法

各目的事業主管機關
個人資料檔案安全維護辦法

***各目的事業主管機關之個人資料檔案安全維護辦法全文，可參閱全國法規資料庫。

全國法規資料庫
https://law.moj.gov.tw/

序	主管機關	法規名稱
9	勞動部	私立職業訓練機構個人資料檔案安全維護計畫及處理辦法
		人力供應業個人資料檔案安全維護計畫及處理辦法
		人力仲介業個人資料檔案安全維護計畫及處理辦法
10	教育部	短期補習班個人資料檔案安全維護計畫實施辦法
		私立兒童課後照顧服務中心個人資料檔案安全維護計畫實施辦法
		私立高級中等以下學校及幼兒園個人資料檔案安全維護計畫實施辦法
		私立專科以上學校及私立學術研究機構個人資料檔案安全維護計畫實施辦法
		運動彩券業個人資料檔案安全維護計畫實施辦法
		海外臺灣學校及大陸地區臺商學校個人資料檔案安全維護計畫實施辦法

各目的事業主管機關個人資料檔案安全維護辦法

***各目的事業主管機關之個人資料檔案安全維護辦法全文，可參閱全國法規資料庫。

全國法規資料庫
https://law.moj.gov.tw/

序	主管機關	法規名稱
11	金融監督管理委員會	金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法
12	大陸委員會	大陸委員會指定非公務機關個人資料檔案安全維護辦法
13	僑務委員會	僑務委員會指定特定非公務機關個人資料檔案安全維護辦法
14	核能安全委員會	游離輻射設備製造業個人資料檔案安全維護管理辦法
15	行政院公共工程委員會	工程技術顧問業個人資料檔案安全維護計畫及處理辦法
16	中央銀行	票據交換所個人資料檔案安全維護計畫標準辦法
17	公平交易委員會	多層次傳銷業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作業辦法
18	國家通訊傳播委員會	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





這樣做就對了！

中小企業對客戶的個人資料保護手冊

個人資料保護委員會籌備處 —— 編著
Preparatory Office of the Personal Data Protection Commission