個人資料保護法主要規範 暨 查核重點分享

分享人：張志洵 Charlie
mpcc.charlie@gmail.com

分享大綱

- 個資法沿革 與 特色
- 個資法架構 與 主要規範
- BS10012簡介
- TPIPAS簡介
- 稽核重點探討

沿革與修法特色

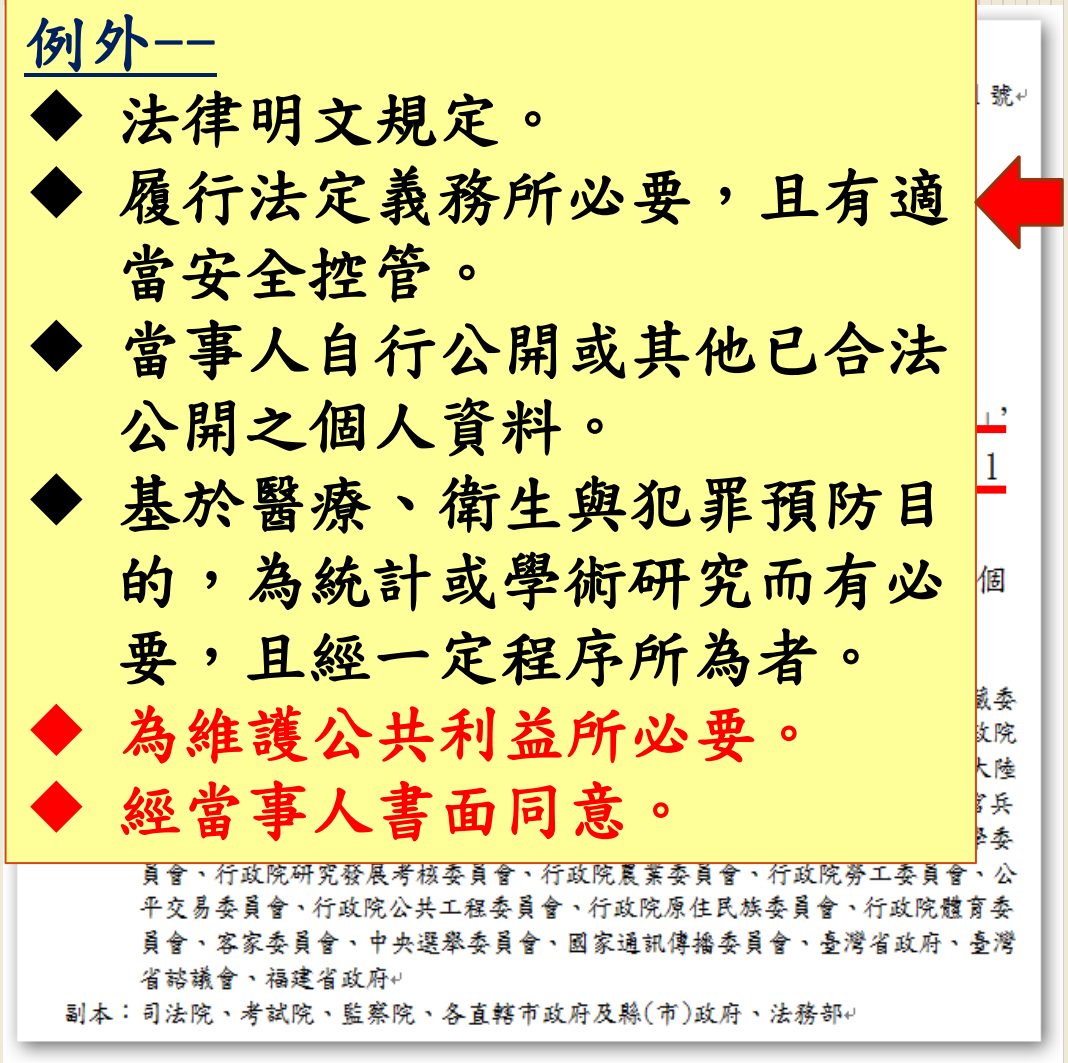
沿革(1/2)

- 84.08.11
- 電腦處理個人資料保護法公布實施
- 99.04.27
- 個人資料保護法立法院三讀通過
- 99.05.26
- 個人資料保護法公布
- 101.09.26
- 個人資料保護法施行細則發布
- 101.10.1
- 個人資料保護法施行

沿革(2/2)

例外--

- 法律明文規定。
- 履行法定義務所必要，且有適當安全控管。
- 當事人自行公開或其他已合法公開之個人資料。
- 基於醫療、衛生與犯罪預防目的，為統計或學術研究而有必要，且經一定程序所為者。
- 為維護公共利益所必要。
- 經當事人書面同意。


員會、行政院研究發展考核委員會、行政院農業委員會、行政院勞工委員會、公平交易委員會、行政院公共工程委員會、行政院原住民族委員會、行政院體育委員會、客家委員會、中央選舉委員會、國家通訊傳播委員會、臺灣省政府、臺灣省諮議會、福建省政府
副本：司法院、考試院、監察院、各直轄市政府及縣(市)政府、法務部

第6條：醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用

第54條：本法修正施行前非由當事人提供之個人資料，依第9條規定應於處理或利用前向當事人為告知者，應自本法修正施行之日起一年內完成告知

本法特性(1/3)

1

擴大保護客體

納入人工與其它所有類型之個人資料與檔案

所謂的個人資料檔案指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

2

普遍適用主體

自然人/法人/公務、非公務機關均適用

適用在中華民國領域外對中華民國人民個人資料蒐集、處理或利用；例外情形規範於51條：

- 自然人為單純個人或家庭活動之目的。
- 公開場所或公開活動中蒐集之未與其他個人資料結合之影音資料

本法特性(2/3)

3

增修行為規範

增加行政裁罰

除加重刑事責任、提高民事損害賠償總額外，針對特定行為，如告知義務、書面同意等，若未制定對應作法，則可能遭受行政罰緩，還能對負責人(代表人, 管理人)加以裁罰監督責任

4

強化行政監督

主管機關之強制檢查

中央目的事業主管機關或直轄市、縣(市)政府若懷疑有問題時，可以執行強制檢查，並扣留或複製可為證據之資料或檔案，並得為禁止、命令刪除、沒入或銷毀、公佈違法情形之處份

本法特性(3/3)

5

促進民眾參與

建立團體訴訟機制

損害之當事人達20人以上，得以書面授與訴訟實施權之方式，委託符合要件之財團法人或公益社團法人，以該法人名義提出團體訴訟，如此可增加民眾的參與，共同監督企業

6

調整責任內涵

舉證責任倒置

一旦發生權訴訟案件，企業得自行舉證無故意或或過失違責任，證明個資外洩非其所造成，否則即需負損害賠償之責。

個資法架構與主要規範

個資法架構

第一章　總則（第1條至第14條）

- 目的 / 定義 / 當事人權利 / 委外/個人資料的蒐集、處理與利用原則 /特種個人資料/書面同意 /當事人告知 /答覆當事人查詢、提供閱覽或複製本/ 個人資料的正確性/個資違法事件通知/回覆當事人權利行使/費用收取

第二章　公務機關對個人資料之蒐集、處理與利用（第15條至第18條）

- 特定目的內/特定目的外/個人資料持有資訊之公開/個人資料檔案之安全維護事項

第三章 非公務機關對個人資料之蒐集、處理與利用（第19條至第27條）

- 特定目的內/特定目的外/國際傳輸/行政檢查/違反個資法之行政處分/行政檢查結果公布/個人資料檔案之安全維護事項

第四章 損害賠償及團體訴訟（第28條至第40條）

第五章 罰則（第41條至第50條）

第六章 附則（第50條至第56條）

定義與原則

個資類別，共計134類

特定目的，共計182類

自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式是識別該個人資料

〇〇六　工業行政

個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯

〇一二　公共衛生或傳染病防治

定義與原則

個資類別，共計134類

特定目的，共計182類

自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式是識別該個人資料

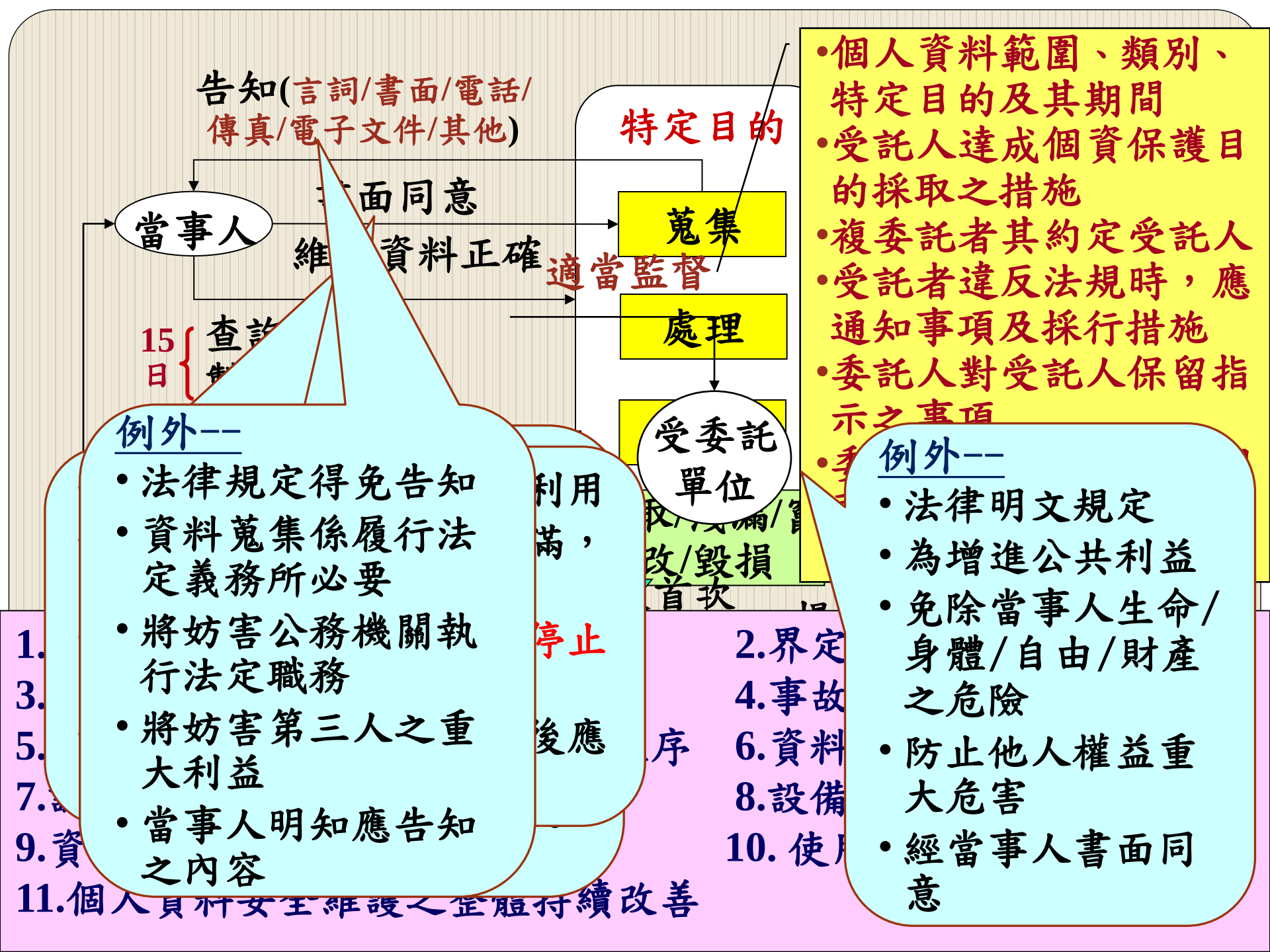
〇〇六　工業行政

個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯

〇一二　公共衛生或傳染病防治

個人資料有關的活動

蒐集	• 指以任何方法取得個人資料。
處理	• 指為建立或利用個人資料檔案所為資料的記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
利用	• 指將蒐集的個人資料為處理以外的利用。
國際傳輸	• 將個人資料作跨國(境)之處理或利用。


告知(言詞/書面/電話/傳真/電子文件/其他)
特定目的
當事人
面同意
維 資料正確
適當監督
蒐集
處理
受委託單位
15日
查詢
利用
滿，
改/毀損
首次
停止
後應
序
1.
2.界定
3.
4.事故
5.
6.資料
7.
8.設備
9.資
10. 使
11.個人資料安全維護之整體持續改善
例外--
• 法律規定得免告知
• 資料蒐集係履行法定義務所必要
• 將妨害公務機關執行法定職務
• 將妨害第三人之重大利益
• 當事人明知應告知之內容
•個人資料範圍、類別、特定目的及其期間
•受託人達成個資保護目的採取之措施
•複委託者其約定受託人
•受託者違反法規時，應通知事項及採行措施
•委託人對受託人保留指示之事項
例外--
• 法律明文規定
• 為增進公共利益
• 免除當事人生命/身體/自由/財產之危險
• 防止他人權益重大危害
• 經當事人書面同意

違反個資法的罰則-民事責任

- 不易或不能證明其實際損害額時，以每人每一事件新臺幣五百元以上二萬元以下計算。但能證明其所受之損害額高於該金額者，不在此限。(第28條第3,5項)
  (取決於對個資的蒐集程度 -> 最小限度蒐集與利用)
- 同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限，但所涉利益超過新臺幣二億元者，以該所涉利益為限。(第28條第4項)
- 非公務機關違反本法，致個人資料遭不法蒐集、處理與利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。(第29條)
  (過失責任之舉證責任倒置)

違反個資法的罰則-刑事責任

第41條

非法蒐集特種資料、違反蒐集、處理、利用、國際傳輸

意圖營利

足生損害於他人者

2年有期徒刑20萬元罰金

5年有期徒刑100萬元罰金

（非告訴乃論）

對公務機關

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

對個資檔案非法變更、刪除或其他妨害資料檔案正確

足生損害於他人者

5年有期徒刑100萬元罰金

違反個資法的罰則-行政裁罰

第47條

違反蒐集特種資料、違反蒐集/處理/利用、國際傳輸規定之處分 → 主管機關 → 5~50萬元罰鍰，並限期改正 → 屆期未改正，按次處罰

雙罰 (1)企業 (2)企業之代表人、管理人或其他有代表權人

第48條

未告知、違反當事人行使權利、正確性與行銷原則、沒有個資檔案安全維護或業務終止後處理計畫

第49條

規避、妨礙或拒絕檢查

→ 主管機關 → 限期改正 → 屆期未改正，按次處2~20萬元罰鍰

→ 2~20萬元罰鍰

BS10012 簡介

概述

- BS10012為英國標準協會基於世界經濟合作暨發展組織(OECD)與亞太經濟合作會議(APEC)對隱私保護的相關要求所發展之國家標準，亦是廣為國際認可的個人資訊管理標準。
- 本標準目的在使組織能實現一個對資料保護法規與優良實務提供維護與改善遵循架構的個人資料保護系統。
  The objective of this Standard is to enable organizations to put in place a personal information management system (PIMS) which provides a framework to maintaining and improving compliance with data protection legislation and good practice.
- 採用P-D-C-A循環，任何規模與區域的組織均可使用。

OECD,APEC,BS10012隱私原則

BS10012主要架構(1/2)

Effect on：31 May 2009

0. Introduction

0.1 PIMS/0.2 Data protection principles/0.3

1. Scope

2. Terms, definitions and abbreviations

2.1 Terms and definitions/2.2 Abbreviation

3.用語與定義

To plan for the implementation of a PIMS that will provide direction and support for compliance with data protection legislation and good practice.

3.1 Establishing and managing the PIMS/3.2 Scope and objective of the PIMS/3.3 Personal information management policy/3.4 Policy content/ 3.5 Responsibility and accountability/3.6 Provision of resources/3.7 Embedding the PIMS in the organization's culture

BS10012主要架構(2/2)

4. Implementation and operating the PIMS

4.1 Key appointments / 4.2 Identifying and recording uses of personal information / 4.3 Training and awareness / 4.4 Risk assessment / 4.5 Keeping PIMS up-to-date / 4.6 Notification / 4.7 Fair and lawful processing /4.8 Processing personal information for specified purposes / 4.9 Adequate, relevant and not excessive / 4.10 Accuracy / 4.11 Retention and disposal / 4.12 Individuals' rights / 4.13 Security issues / 4.14 Transfer of personal information outside the EEA / 4.15 Disclosure to third parties / 4.16 Sub-contracted processing /4.17 Maintenance

5. Monitoring and reviewing the PIMS

5.1 Internal audit / 5.2 Management review

6. Improving the PIMS

6.1 Preventive and corrective actions / 6.2 Continual improvement

BS10012

臺灣個人資料保護與管理制度規範(TPIPAS)

資料來源：臺灣個人資料保護與管理制度網站

http://www.tpipas.org.tw

依據

- 2008年立法院第7屆第1會期第15次會議決議：為保障民眾個人隱私建議政府參考國外作法，推動我國隱私權管理保護認證制度。案經行政院2008年9月3日交經濟部研議協助民間產業建立個人資料保護管理系統標準與隱私權標章驗證制度。
- 2009年8月行政院「塑造資安文化、推升資安產值」產業科技策略會議，決議推動電子商務個人資料管理暨資訊安全行動方案。
- 2009年12月行政院核定「塑造資安文化、推升資安產值」關鍵推動方案（99年至102年），推動TPIPAS即為該方案行動計畫之一。

TPIPAS制度規範 (1/2)

版 次：2012 V.1
公告施行日期：2012年09月04日

0.前言

0.1 概述/0.2 訂定目的/0.3 用途/0.4 PDCA方法論

1.適用範圍

針對蒐集、處理、利用及國際傳輸個人資料之事業，訂定相關規範事項，以建立PIMS，確保個人資料之安全

2.版本標示

引用本制度規範，應註明所引用版本。若未註明者，則指使用最新版本

3.用語與定義

個人資料管理制度/個人資料/當事人/事業/個人資料管理代表/個資管理人員/事業人員/事故

4.要求事項

4.1 一般要求事項/4.2 個人資料保護管理政策/4.3 個人資料保護管理手冊/4.4 個別要求事項/4.5 管理制度之實施/4.6 教育訓練

TPIPAS制度規範 (2/2)

5.管理責任

5.1 最高管理階層/5.2 管理代表/5.3 個資管理人員

6.有效性量測

應針對個人資料管理制度之實施，建立分析量測機制，以確保制度之持續有效運作

7.文件及紀錄之控管

7.1 文件及紀錄之範圍/7.2 文件管理/7.3 記錄管理

8. 內部評量

每年應依其特性規劃執行內部評量，是否(1) 符合法規及本制度之要求；(2) 符合個人資料保護管理政策、手冊及相關具體規則之要求

9. 改善

9.1 定期檢視/9.2 矯正及預防措施

TPIPAS

取得標章之事業

2014年10月15日

統一超商
股份有限公司

全家便利商店
股份有限公司

康迅數位整合
股份有限公司

欣亞數位
股份有限公司

博客來數位科技
股份有限公司

台灣樂天市場
股份有限公司

香港商雅虎資訊
股份有限公司

亞東電子商務
股份有限公司

特力屋
股份有限公司

特力屋室內裝修設計
股份有限公司

臺灣集中保管
結算所

統一資訊
股份有限公司

日翊文化行銷
股份有限公司

稽核重點探討

配置管理人員及相當資源

- 針對個資之保護與管理是否已定義明確的分工權責與角色職掌，包含：
  - 常態編組或組織分工
  - 最高管理階層指派之資深管理代表
  - 部門(系統)資料保護代表
  - 日常作業之負責人員
- 針對個資之保護與管理是否已規劃或配置適當之資源，包含：
  - 現有資源之統計與紀錄
  - 後續所需必要資源之規劃與經費編列

界定個人資料之範圍

- 確認是否已針對組織自行或委託第三方蒐集、處理與利用之各類個人資料檔案，完成清查與造冊列管，並辨識相關個資檔案之敏感程度
- 確認是否已針對各類個人資料相關之適用法令、規定完成清查確認
- 確認是否已整理出各類個人資料檔案蒐集、處理、利用之作業流程
- 確認是否建立與執行定期/不定期個資檔案、適用法規與作業流程變更時之複查與更新程序或方法

個人資料之風險評估及管理機制

- 確認是否已針對組織所持有之個人資料進行相關威脅辨識與風險評估
- 確認是否已根據不同個資檔案之敏感性、威脅情境與風險等級訂定相關之風險對策與安全管控措施
- 確認是否已將相關威脅辨識、風險評估風險對策與安全管控措施之結果彙整為紀錄文件或建立資料庫
- 確認是否已建立與執行定期或與個資盤點清冊更新連動的不定期個資風險評估與管理程序或方法

事故之預防、通報及應變機制

- 確認是否已明確定義事故發生時之應變分工與權責，以及緊急處置原則
- 確認是否已建立事故發生之內外部通報流程(包含通報名冊與緊急連絡方式)
- 確認是否已建立並執行事故發生後之調查與改善追蹤機制
- 確認是否已預劃事故發生後通知當事人之管道、方式與期限

蒐集/處理/利用內部管理程序–管理原則

- 評估各類個資蒐集之必要性與合理性
- 分析是否符合資料蒐集最小原則
- 評估各類個資保存年限之適當性
- 確認是否已建立並執行個資複製、影印與列印之管制與管理程序與方法
- 確認是否已建立並執行新增個資檔案蒐集之審查與核定程序與方法
- 確認是否已規劃對內/對外公布個人資料 之規範與要求

蒐集/處理/利用內部管理程序–權利行使

- 確認是否已針對各類個資之權利行使建立並執行相關受理方式、窗口，以及受理與回覆相關作業程序
- 確認受理程序中，是否包含申請人身分驗證機制(當事人本人或其授權之代理人)
- 確認受理更正或補充資料時是否要求提供必要之證明
- 評估現有受理與回覆程序，是否可達成於法定期限內(15/30天)回覆當事人之要求
- 抽查受理申請案件中，未於法訂期限回覆者，是否於法定期限內先將原因通知當事人，並於法訂延長期限內完成回覆

蒐集/處理/利用內部管理程序–特定目的

- 確認各類個資檔案之蒐集是否均已明確訂定其目的
- 抽查各類個資檔案適實際利用情形，評估是否均屬該資料特定目的之必要範圍
- 確認是否已建立與執行特定目的外利用的申請與審核程序或方法

蒐集/處理/利用內部管理程序–告知義務

- 評估各類個資檔案蒐集告知內容是否符合法令要求
- 評估各類個資檔案蒐集告知之方式是否足以使當事人知悉或可得 知悉，或留有紀錄
- 針對未於蒐集時進行告知之各類個資檔案，評估其是否符合個資法八條二項規定之得免告知條件
- 確認持有之各類個資檔案中，是否有非由當事人提供之情形，若有，則應先確認該蒐集是否符合個資法十九條一項之條件，並確認是否於資料中有相關註記

蒐集/處理/利用內部管理程序–書面同意

- 評估各類個資檔案蒐集是否符合個資法十九條一項條件之一
- 評估經當事人書面同意者，其同意書之保存及保管方式是否適當，並進行抽查確認

蒐集/處理/利用內部管理程序–拒絕行銷

- 確認用於行銷之個資是否已明列於該個資蒐集之特定目的之一
- 確認是否已建立並執行當事人拒絕利用個資行銷之免費受理方式、窗口
- 確認受理當事人拒絕行銷後，當事人個資紀錄上是否已有明確之註記或有其他限制行銷利用之機制

蒐集/處理/利用內部管理程序–刪除銷毀

- 確認個資之刪除與銷毀是否包含相關備份與複製資料
- 抽查已屆年限或特定目的消失之個人資料是否已確時刪除銷毀
- 確認個資之刪除與銷毀是否保持完整之紀錄

蒐集/處理/利用內部管理程序–國際傳輸

- 確認組織持有之個人資料是否有傳送國外之情形，若有，則進行以下評估：
  - 傳送之資料是否涉及國家重大利益或國際條約或協定(**如OECD或APEC**)有特別規定者
  - 接受國是否有類似之個人資料保護法規
  - 接受國是否有將相關資料再傳送給其他無類似法規之國家

資料安全管理與人員管理

- 確認相關安全控制機制是否已涵蓋現有不同敏感程度與保存型態之個人資料媒體(如紙本、硬碟系統檔案、光碟...等)
- 確認現有安全管控機制至少包含以下必要控制：
  - 保存與操作處理
  - 內外部傳輸、交換
  - 存取控制(權限與認證管控，調離職/職務異動權限變更)
  - 使用規範(如螢幕保護、桌面清空、匯出/匯入)
  - 防毒/防駭/防竊
  - 人員保密協定與日常作業考核
- 評估以上必要控制之適足性(參考ISO 27000系列規範)

認知宣導及教育訓練

- 確認組織已針對個資保護與管理提供必要之宣導、訓練(宣導資料、教材與課程規劃)
- 確認所有個資保護與管理之日常作業負責人員是否均已完成訓練或取得宣導資料
- 抽核日常作業負責人員是否了解相關作業程序與規範

設備安全管理

- 確認相關安全控制機制是否已涵蓋存放或處理現有各種不同個人資料媒體型態之設備
- 確認現有安全管控機制是否已適當評估以下控制：
  - 場域安全管理：如門禁管制設施、人員/物品進出管制、保全設施、場內作業安全規範、環控與防災設施、開放區域的安全管理
  - 設備實體管理：如設備放置安全、電力或其他輔助設施之安全、線路安全、設備維護、場域外之設備安全、設備處置/送修/再利用之安全、財產的移除
- 評估以上採行控制之適足性(參考ISO 27000系列規範)

資料安全稽核機制

- 評估現有資料安全稽核之頻率與範圍之適足性，並且是否明確的將高風險之個資納入查核
- 確認執行之稽核人員是否具備相當之職能
- 確認是否針對稽核所見缺失之改善進行追蹤管控

使用紀錄、軌跡資料及證據保存

- 確認是否已規範並執行高敏感或高風險之個人資料的使用軌跡(如資料建檔、異動，查詢/調閱、匯出/列印/複印、外部傳輸/交換，以及刪除/銷毀等)之紀錄/資料格式與查詢介面設計
- 評估相關使用軌跡之紀錄/資料保存方式與期限之適當性

個人資料安全維護之整體持續改善

- 確認是否已建立並執行個資安全定期檢討機制
- 確認期間內發生之安全事故、稽核結果、風險評量與監控結果、程序審查、技術更新、日常作業負責人之回饋，以及客訴案件等是否納入前述定期檢討機制中進行檢視
- 確認是否已針對前述檢視結果採取相關預防與矯正措施

對受託者適當之監督

- 廠商評選階段：確認受託者與其複委託者是否具有相關安全認證，或已由委託單位事先完成審查確認其已依施行細則12條二項要求採取適當之安全措施
- 合約訂定階段：確認合約內容是否明確訂定以下事項：
  - 個人資料之範圍、類別、特定目的及其期間
  - 受託者違反法令時，應通知之事項及採行補救措施
  - 保留指示之事項
  - 委託終止或解除時，載體返還與持有資料刪除規範
- 委託執行階段：是否定期確認受託者執行狀況，並記錄確認結果
- 委託結束階段：評估委託單位如何確認受託者已確實刪除相關資料

Discussion

個人資料之類別

特徵類

C〇一一 個人描述

例如：年齡、性別、出生年月日、出生地、國籍、聲音等

C〇一二 身體描述

例如：身高、體重、血型等

C〇一三 習慣

例如：抽煙、喝酒等

C〇一四 個性

例如：個性等之評述意見。

家庭情形

C〇二一 家庭情形

例如：結婚否、配偶/同居人姓名、結婚日期、子女人數等

C〇二二 婚姻之歷史

例如：前次婚姻、離婚或同(分)居細節及相關人姓名等

C〇二三 家庭成員細節

例如：子女、受扶養人、家庭其他成員或親屬及旅居國外及大陸人民親屬等

C〇二四 其他社會關係

例如：朋友、同事及其他家庭以外之關係等

個人資料之特定目的

員工個資相關之特定目的

代號	特定目的項目
○○一	人身保險
○○二	人事管理(包含甄選、離職及所屬員工基本資訊、現職、學經歷 、考試分發、終身學習訓練進修、考績獎懲、銓審、薪資待遇、 差勤、福利措施、褫奪公權、特殊查核或其他人事措施)
○三一	全民健康/勞工/農民/國民年金或其他社會保險
○三六	存款與匯款
○六三	非公務機關依法定義務所進行個人資料之蒐集處理及利用
○六九	契約、類似契約或其他法律關係事務
一○九	教育或訓練行政
一一○	產學合作
一一四	勞工行政
一一九	發照與登記