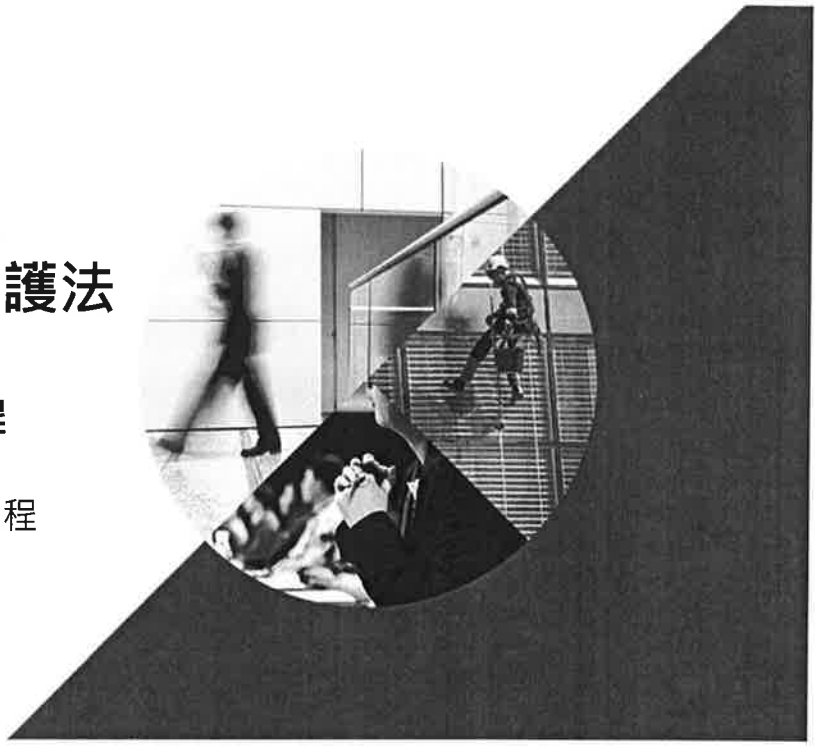
bsi.

公務機關如何因應 個人資料保護法

2017
個人資料保護教育訓練課程

PIMS ESS Training Course
個人資訊管理系統基礎訓練課程



章鈺　先生
(Mr. Oscar Chang)

BSI 英國標準協會
BSI Taiwan,
Client Manager 客戶經理
BS10012 產品經理
ISO 29100 產品經理

學歷：
- 政治大學 法律碩士
- Baker University, Kansas, U.S.A 管理科學碩士
- 輔仁大學 資訊管理學士

稽核經歷：
- 總統府、行政院、行政院人事總處、行政院主計總處、行政院研考會、考試院、考選部、證交所、期交所、櫃買中心、集保結算所、票交所、財金資訊、聯合信用卡中心、聯合徵信中心、中華電信、遠傳電信、臺灣積體電路、聯華電子、教育部電算中心、Accenture、NIKE、華碩雲端、阿里雲、台北富邦、彰化銀行、台新銀行、群益證券、元富證券、遠雄人壽、安達人壽等。

IT專業領域：
- 開放式作業系統管理/ 資料庫管理/ 應用系統軟體程式開發、系統分析/ SAP 系統管理

稽核資格：
- IRCA ISO 27001 主導稽核員
- ISO 22301 主導稽核員
- BS 10012 主導稽核員
- ISO 29100 主導稽核員
- ISO 20000 稽核員

稽核員相關專業證照：
- ISACA CISA/ CISM/ CGEIT/ CRISC Certified

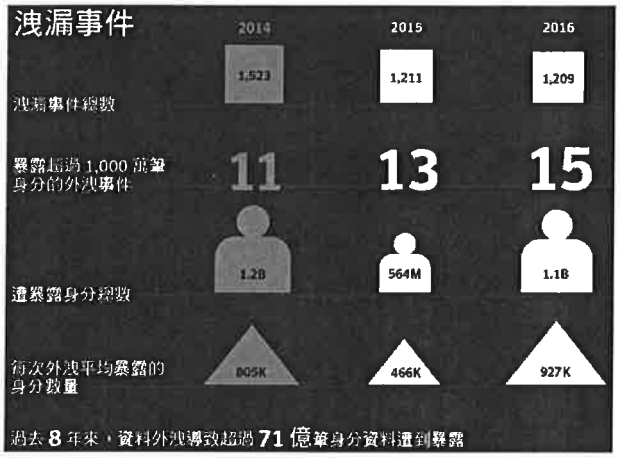
課程大綱

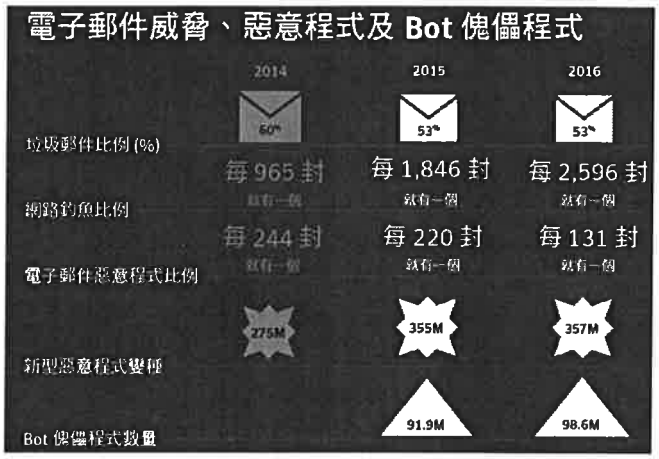
- 新知分享
- 2015年新修個人資料保護法
- 從法院判決書看個人資料保護法要求
- 近期個資事故新聞檢視應有安全作為
- Q&A

新知分享

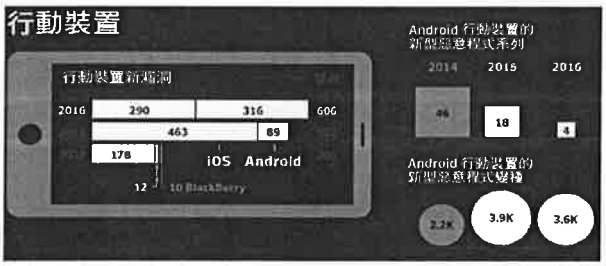
bsi.

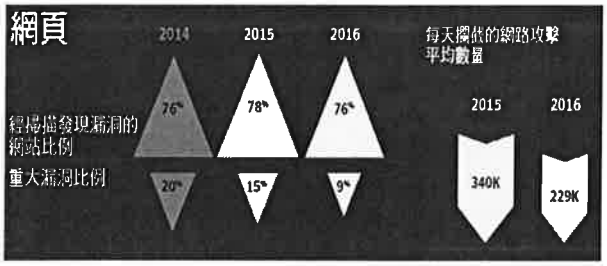
Symantec 2017 網路安全威脅研究報告

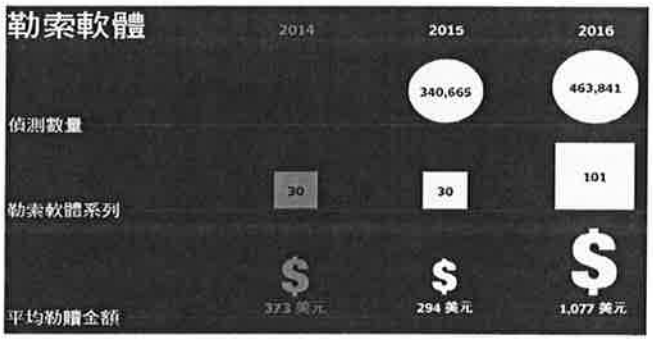




Symantec 2017 網路安全威脅研究報告







Symantec 2017 網路安全威脅研究報告

2016 年資料外洩十大原因

資料竊取是 2016 年資料外洩主要原因的第一名，比例超過 1/3。

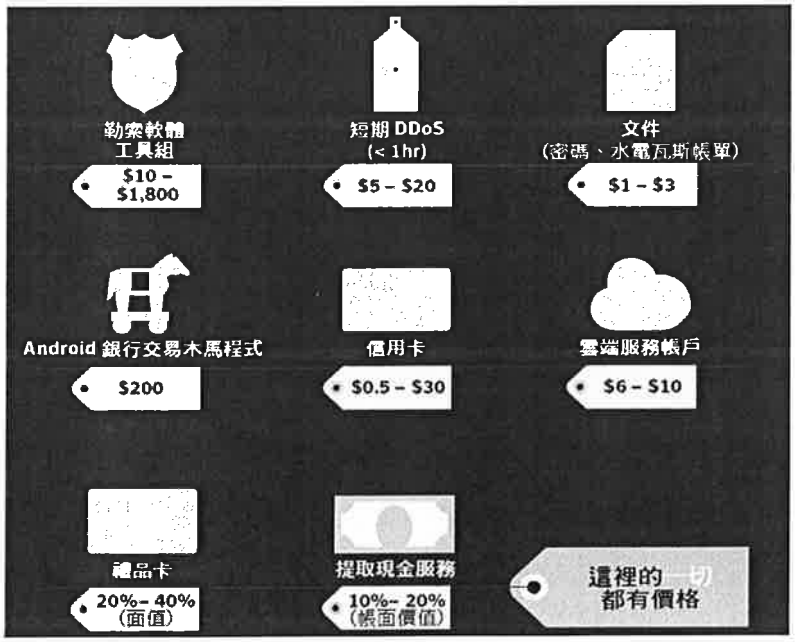
排行	原因	2015 年 (%)	2016 年 (%)	百分點變異
1	資料竊取	42.4	36.2	-6.2
2	使用資料不當	20.4	19.3	-1.1
3	未分類或其他原因	11.9	19.2	7.3
4	網路釣魚、詐騙或社交工程	21.8	15.8	-6.0
5	意外資料遺失	1.7	3.2	1.5
6	裝置遺失或遭竊	0.6	3.1	2.5
7	IT 錯誤導致資料遺失	0.5	1.6	1.1
8	網路破壞或 DDoS	0.3	1.6	1.3
9	敲詐、勒索或破壞	0.1	0.2	0.1
10	身分竊取或詐騙	0.1	0	-0.1

依據資安事端數量的十大資料外洩部門

2016 年最受資料外洩影響的產業為服務業。

排行	行業	洩漏事件	百分比
1	服務業	452	44.2
2	金融、保險及不動產業	226	22.1
3	製造業	116	11.3
4	零售業	84	8.2
5	運輸及公用事業	75	7.3
6	批發業	32	3.1
7	建築業	20	2.0
8	採礦業	8	0.8
9	公共行政	6	0.6
10	無法分類的機構	3	0.3

Symantec 2017 網路安全威脅研究報告



Symantec 2017 網路安全威脅研究報告

資料外洩數量前十名國家

美國在 2016 年是受到資料外洩影響最大的國家。

排行	國家/地區	洩漏事件
1	美國	1023
2	英國	38
3	加拿大	19
4	澳洲	15
5	印度	8
6	愛爾蘭	8
7	日本	7
8	以色列	6
9	德國	5
10	泰國	5

地下經濟市集定價表

支付卡	價格
單一信用卡	0.5 - 30 美元
單一信用卡含完整詳細資料 (Fullz)	20 - 60 美元
轉儲磁條磁軌 1&2 及 PIN	60 - 100 美元
轉帳服務	
提取現金服務	10% - 20%
帳戶	
線上銀行帳戶	帳戶餘額的 0.5% - 10%
零售商帳戶	20 - 50 美元
雲端服務供應商帳戶	6 - 10 美元
身分	
身分 (姓名、SSN 及 DOB)	0.1 - 1.5 美元
掃描護照及其他文件 (例如水電瓦斯帳單)	1 - 3 美元

2015年12月新修
個人資料保護法

bsi.

重新定義特種個資及合法蒐集處理利用成立條件

第六條

- 有關**病歷**、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。但有下列情形之一者，不在此限：
  - 一. 法律明文規定。
  - 二. 公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且**事前或事後**有適當安全維護措施。
  - 三. 當事人自行公開或其他已合法公開之個人資料。
  - 四. 公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
  - **五. 為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內且事前或事後有適當安全維護措施。**
  - **六. 經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。**
- 依前項規定蒐集、處理或利用個人資料，準用**第八條、第九條規定**；其中前項第六款之書面同意，**準用第七條第一項、第二項及第四項規定，並以書面為之。**

合法蒐集處理個人資料成立條件

第五條

- 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**。

第十五條

- 公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，**應有特定目的**，並符合下列情形之一者：
  - 一. 執行法定職務必要範圍內。
  - 二. 經**當事人同意**。
  - 三. 對當事人權益無侵害。

合法將個人資料作為目的範圍外利用之成立條件

第十六條

- 公務機關對個人資料之利用，除第六條第一項所規定資料外，應於**執行法定職務必要範圍內為之**，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：
  - 一. 法律明文規定。
  - 二. 為維護國家安全或增進公共利益所必要。
  - 三. 為免除當事人之生命、身體、自由或財產上之危險。
  - 四. 為防止他人權益之重大危害。
  - 五. 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
  - 六. 有利於當事人權益。
  - 七. 經**當事人同意**。

直接蒐集個人資料時得免除告知成立條件

第八條

- 公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項 (以下略)
- 有下列情形之一者，得免為前項之告知：
  - 一. 依法律規定得免告知。
  - 二. 個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
  - 三. 告知將妨害公務機關執行法定職務。
  - 四. 告知**將妨害公共利益**。
  - 五. 當事人明知應告知之內容。
  - **六. 個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。**

個資法實施前對先前間接蒐集個人資料時告知要求

第五十四條

- 本法中華民國九十九年五月二十六日修正公布之條文施行前，非由當事人提供之個人資料，於本法一百零四年十二月十五日修正之條文施行後為處理或利用者，應於處理或利用前，依第九條規定向當事人告知。
- 前項之告知，得於本法中華民國一百零四年十二月十五日修正之條文施行後首次利用時併同為之。
- 未依前二項規定告知而利用者，以違反第九條規定論處。：

當事人同意蒐集或目的外利用個人資料時之要求

第七條

- 第十五條第二款及第十九條第一項第五款所稱**同意**，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。
- 第十六條第七款、第二十條第一項第六款所稱**同意**，指當事人經蒐集者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。
- 公務機關或非公務機關明確告知當事人第八條第一項各款應告知事項時，當事人**如未表示拒絕，並已提供其個人資料者，推定**當事人已依第十五條第二款、第十九條第一項第五款之規定表示同意。
- 蒐集者就本法所稱經當事人同意之事實，**應負舉證責任**。

個人資料正確與保留期限要求

第十一條

- 公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。
- 個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須，或經當事人書面同意，**並經註明其爭議者**，不在此限。
- 個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。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。
- 違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。
- 因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。

違反個人資料保護法刑事責任

第四十一條

- **意圖為自己或第三人不法之利益或損害他人之利益，而**違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處五年以下有期徒刑，**得併**科新臺幣**一百萬元**以下罰金。

第四十五條

- 本章之罪，須告訴乃論。但犯**第四十一條**之罪者，或對公務機關犯第四十二條之罪者，不在此限。

特定目的與個人資料類別參考

第五十三條

- 法務部**應**會同中央目的事業主管機關**訂定特定目的及個人資料類別，提供公務機關及非公務機關參考使用。**

從法院判決書看
個人資料保護法要求

bsi.

1 高等法院臺南分院105年上易字第 393 號刑事判決

案由：

- 甲○○明知行動電話號碼屬於個人資料保護法第2 條第1 款所定之個人資料，非公務機關對於其利用應於特定目的之必要範圍內為之，詎甲○○竟基於非法利用個人資料之犯意，於民國103 年11月中旬，在其位於臺南市○區○○里○○路 0 段000巷00弄00號6 樓住處，利用電腦設備上網連結網際網路，登入00聊天室與網友聊天，並接續**將乙○○所有行動電話門號0000000000號散布予2 名網友**，以此方式非法利用乙○○之個人資料，足生損害於乙○○個人之隱私權，並**致乙○○之行動電話號碼為00聊天室網友所取得，而分別撥打電話或傳送簡訊予乙○○**，相約其性交，令乙○○不堪其擾。嗣經乙○○報警，經警循線查悉上情。

結論：

- 原判決(臺灣臺南地方法院105 年度易字第103 號中華民國105 年5 月2 日第一審判決)撤銷

1 高等法院臺南分院105年上易字第 393 號刑事判決

甲○○主張：

- 行動電話號碼全然不具備識別性，尚須結合其他資訊始能識別特定之個人；同一行動電話門號前後可能有多人接續使用，與使用人間之關聯性較為薄弱。
- 本件除告訴人之指述外，僅有告訴人提供之自己於103 年12月間與不特定第三人之對話紀錄，非但時間上不相符合，且對話紀錄亦無指明被告甲○○有任何違反個人資料保護法之犯行。
- 「○」、「00000 」、「○○○○」、「0000」等暱稱IP登入記錄檔並非全為被告甲○○所使用之固定IP 位址，顯見上開暱稱並非被告甲○○所專屬專用，且以告訴人與他人之對話紀錄，均無法特定到底係何人公開告訴人之手機門號，實無法證明被告涉有違反個人資料保護法之犯行。
- 又與告訴人對談之人多誤認告訴人為女性，更可證明僅告知行動電話號碼並無法特定個人之身分資訊云云

1 高等法院臺南分院105年上易字第 393 號刑事判決

承審法官認為：

- 選任辯護人雖辯稱行動電話號碼不具識別性，諸如身份證字號僅為一連串數字之組成，指紋亦為生理圖像，如僅以「透過一連串數字組成並不足以識別特定之人」區別是否為個人資料保護法所規範之個人資料，**無異架空該法保護個人人格權之意旨**。

- 手機通訊於現代人日常生活中重要性日增，而行動電話號碼之變更對於現代人而言亦造成甚多不便，電信業者亦衍生可攜碼服務，即係為避免號碼變更所造成不便；實難以行動電話號碼得以任意變更或終止使用，**即否定其對於使用之專屬性及獨特性**。再者，號碼之持有人於當時僅有1 人，以其為憑據**直接即可與該人連結而識別出特定個人**。

- 被告另辯稱僅以私訊方式傳送告訴人行動電話號碼予2 人，**並未公開**於00聊天室予不特定人知悉，惟被告將行動電話號碼傳送予他人時，即已觸犯不當利用個人資料罪，此與其以私訊或公開方式傳送予特定人或不特定之公眾均無涉。

2 高等法院 105 年金上訴字第 5 號刑事判決

案由：

- 被告等4 人係渣打銀行臺北電話行銷部門員工，均負責行銷信用卡及信用貸款予渣打銀行既有客戶之業務。被告等4 人於民國101 年6 月15日均與渣打銀行簽訂聘僱合約、資料維護及隱私聲明、渣打銀行業務人員工作準則、絕不容許行為清單。詎被告等4人竟共同意圖為自己不法之利益及意圖營利，基於無故洩漏業務上知悉工商秘密之犯意聯絡，於101 年下半年起至102 年4 月間止，在臺北電話行銷部門上址，利用業務期間瀏覽渣打銀行電腦系統客戶資料之機會，以其等所有之行動電話照相機將客戶基本資料拍攝成照片，再以行動電話通訊軟體Line、WhatsApp等將上開照片傳送，作為延攬汽車貸款業務使用，並取得回扣。

結論：

- 原審以本案不能證明被告無罪之諭知，於法核無違誤。檢察官上訴意旨，未另行積極舉提具體事證，徒就已經原審詳予論述之證據資料再事爭執，任意指摘原判決不當，求予撤銷改判，為無理由，應予駁回。

2 高等法院 105 年金上訴字第 5 號刑事判決

承審法官認為：

- 個人資料保護之目的，乃是避免因濫用當事人資訊而侵害其權益，故凡是針對個人資料之蒐集、處理及利用，必須在合理使用之範圍內始得為之，以避免造成個人人格權受到侵害；反面言之，若資訊之內容不足以造成個人人格權之侵害，甚至根本無法辨識、特定究係何人之資訊，自不在本法保護之範圍內。

- **直接識別性**：不必結合複數以上之個人資料即可特定個人之資料者，例如：姓名、國民身分證統一編號、號碼、指紋，即具有直接識別性，其所代表之單一意義，原則上具有直接識別個人之特徵且具有重要性，其他必須結合複數以上之資料群，始具有直接識別性，因此，若對於資料群之比對，僅提出單一形態或縱使結合複數形態之個人資料，亦不足以表現或特定個人之資料，自無侵害之問題。

- **識別重要性**：針對「可間接識別特定個人」資料之判斷標準，在上開資料群之範圍外，仍須參酌識別特定個人之「關鍵」或「重要性」之多寡，以確立各該間接資料是否對於「特定」個人有其「關鍵」或「重要性」之價值。

2 高等法院 105 年金上訴字第 5 號刑事判決

承審法官認為：

- 被告確有於101年10月1日起至102年4月間多次提供渣打銀行客戶之**電話號碼**，然**並無提供客戶之姓名或其他資料**，已如上述，**客觀上無從令蒐集者得以知悉被提供之客戶之姓名年籍等私人資訊或對外之社會活動狀況**，並進而利用該份資料對照、組合、連結而得識別特定個人，即其既無法藉由「間接連結」之方式，達到足以「直接識別」之結果，自難認屬個人資料保護法所指之個人資料法所指之個人資料。

- 至檢察官上訴意旨固稱：依現今網路技術之進步神速，社交網站之興盛，單一資料、照片透過電腦運算或是網路搜尋方式做交叉比對查詢，可取得更完善之資料，而以同案被告蒐集所得之渣打銀行客戶電話號碼，輸入臉書網站進行查詢，15筆中即有8名電話號碼之人登錄資料於臉書網站上，是電話號碼應為個人保護法所保護之個人資料云云。惟綜全卷，**檢察官並未提出任何其以渣打銀行客戶電話號碼輸入臉書網站進行查詢之相關臉書查詢資料，復經本院單以電話號碼進入搜尋網站或臉書網站查詢，並未能獲得任何個人資料**。故縱被告有上開渣打銀行客戶之電話資料，亦無從成立該法第41條第2項之罪責。

3 高等法院 104 年上字第 1383 號民事判決

上訴人主張：

- 上訴人為○○整型外科診所護士，被上訴人甲○○於102年12月15日在PTT網站Facelift發表「[心得] 診所護士寫手門與沒開收據，涉逃稅」，附檔案下載網址，該檔案有上訴人在○○診所照片。被上訴人乙○○於103年5月13日於臉書開設「整形外科雙眼皮泡泡眼手術失敗心得分享」社區，嗣於該社區登載文章之連結網址。被上訴人共同將**未經伊同意所拍攝之系爭照片登載於網路上供人瀏覽**，侵害肖像權；乙○○蒐集、利用系爭照片，違反個人資料保護法。

- 依民法第18條第1項、第184條、第213條之規定，請求甲○○刪除系爭文章所附照片，乙○○刪除上開文章連結；依民法第18條第2項、第184條、第185條第1項、第195條第1項之規定，請求被上訴人賠償非財產上之損害，另依個人資料保護法第29條、第28條第2項規定，對乙○○為同一之請求等情，求為命甲○○自PTT網站Facelift看板文章，將照片刪除，乙○○將臉書社區登載文章連結刪除，及先位命被上訴人連帶給付新台幣10萬元及自起訴狀繕本送達翌日起加付法定遲延利息，備位命被上訴人各給付5萬元及自起訴狀繕本送達翌日起加付法定遲延利息判決。

3 高等法院 104 年上字第 1383 號民事判決

被上訴人主張：

- 系爭照片非伊所拍攝，而係於○○診所接受手術失敗病人於閱覽網路文章，至○○診所回診時拍攝，再轉交予伊。上訴人隱匿渠等為○○診所之護士身分，於網路撰文為○○診所宣傳、薦證，使消費大眾誤信為一般消費者之推薦，上訴人所為不實行銷行為，顯已違反公平交易法及醫療法規，伊**刊登系爭照片之目的，在使消費大眾藉由比對系爭照片，知悉上訴人乃○○診所設立廣告粉絲頁之寫手，以揭發該診所之不實行銷手法**，避免網友受騙，致整形失敗，係為**增進公共利益，防止他人權益受重大危害**，自得依個人資料保護法第20條第1項第2款、第4款規定阻卻違法。

- 又僅刊登照片供大眾比對，未予後製或醜化，亦**未揭露上訴人其他年籍資料**等，顯**未逾越合理使用必要範圍**，且屬**言論自由保障**之範疇，**符合比例原則**，對上訴人不構成侵權行為等語，資為抗辯。

3 高等法院 104 年上字第 1383 號民事判決

承審法官看法：

- 人格權受侵害時，得請求法院除去其侵害；有受侵害之虞時，得請求防止之。
- 人格權侵害責任之成立以不法為要件，而不法性之認定，**採利益衡量原則**，就被侵害之法益、加害人之權利及社會公益等，**依比例原則而為判斷**；倘**衡量之結果對加害人之行為不足正當化，其侵害始具有不法性**。
- 查乙○○係自他人取得系爭照片而為利用，固為乙○○所自認，然其蒐集、利用系爭照片之目的，係為藉此指明上訴人係○○診所之護士，供有意施行相關整形手術之人，於閱覽上開相關文章、資訊後，**得為正確之判斷及選擇，避免日後發生醫療糾紛，造成權益遭受重大危害**，已如前述，堪認乙○○之行為**與公共利益有關**，且係**為防止他人權益受重大危害**，依前揭規定，難謂其行為不法，是上訴人主張依個人資料保護法第29條、第28條第2項規定，請求乙○○刪除上開登載系爭文章之連結網址，及賠償其非財產上損害，亦有未合。

4 高等法院 105 年訴易字第 6 號民事判決

被告主張：

- 被告於民國100年11月19日某時、 同年月21日某時，在不詳地點，擅自輸入伊身分證號碼等資料，分別侵入下稱慈濟醫院門診預約掛號系統、三總醫院網路預約掛號系統， 查悉伊於100年11月21日慈濟醫院身心醫學科門診掛號， 以及100年11月21日三總醫院胸腔內科門診掛號，竟無故予以取消，致伊無法依原定掛號內容就診。
- 被告擅自輸入伊身分證號碼等個人資料，查悉伊掛號科別、門診時間等，並予取消，符合個人資料保護法第2條第3、4款、第6條所規定，違法蒐集、處理伊醫療個資之行為，爰依個資法第28、第29條規定，請求被告就每一事件各賠償新臺幣（下同）2萬元；個資法屬民法第184條第2項所稱「保護他人之法律」，隱私權又係民法第195條所明定之人格權，爰依民法第184條第2項、第195條規， 請求被告給付伊50萬元之精神賠償。聲明： 被告應給付540,000元及自起訴狀繕本送達翌日起至清償日止，按年息5%計算之利息。

刑事判決：本院104年度上訴字第2594號刑事判決有罪確定。

4 高等法院 105 年訴易字第 6 號民事判決

承審法官看法：

- 被告違反個資法，於慈濟、三總蒐集、處理原告個資，致生損害人格權，應屬二事件，合先敘明。原告就被告上開行為所受之損害，並未提出任何證據證明，經本院行使闡明權，原告亦僅泛稱「刑事卷有相關急診、看診證據」等語。另查：

1. 原告陳稱：被告上開行為， 致未能於三總醫院胸腔內科看診，需以急診方式就醫。急診回家後，當晚又到內湖的醫院住院；慈濟醫院原應看診部分，雖於重新掛號後同日完成看診，但該次身心科門診被取消後，因心情低落割腕， 足認被告違反個資法之上開行為，致所受財產及非財產上之損害，應有「不易或不能證明其實際損害」之情形。

2. 本院審酌：被告因不滿原告提告刑事附帶民事同案被告公開帳戶密碼或任意張貼不雅照片等散布猥褻影像行為，竟無故輸入原告個資，入侵醫院電腦，蒐集原告醫療掛號資料，並為取消掛診，致原告未能依原預定看診療程診治其憂鬱病症；犯後無任何悔意或向原告道歉或與原告達成和解賠償，以及原告103年度所得600元， 名下無任何財產；被告103年度無所得，名下有1997年福特六和汽車一台，有法院依職權調閱之稅務電子閘門財產所得調件明細表，認原告得請求財產及非財產上之損害，每一事件應以5000元為適當，合計得請求10,000元，逾此部分之請求，不應准許。

近期個資事故新聞檢視應有安全作為

bsi.

1 會員資料外洩 勞動部：加強預設密碼複雜度

中國時報 2016.10.26

- 新北市一國際資產管理公司傳出涉嫌入侵勞動部勞動力發展署的「台灣就業通」網站，竊取3萬多筆民眾個資，勞動部勞動力發展署指出，由於這不是網站資安問題，而是預設的簡易密碼被不法人士使用，為了避免類似情況發生，所以未來在預設密碼時，將會使用亂數密碼，也會提醒民眾在登入網站之後變更密碼，以維護個人資料安全。
- 發展署表示，在今年7月間發現有多個會員登錄資料異常，進一步查出是從同一個IP位置登錄，因為懷疑有不當取得資料的可能，便立即封鎖該IP位置、暫時關閉異常的會員帳戶，並立刻將相關資料移送檢調處理。
- 過去為了方便會員使用，會員在建立帳號之後，預設密碼較為簡易，「有些民眾是在實體就業中心辦理帳戶的，雖然現場人員有提醒要更改，但可能民眾回家後沒有馬上更改」，透過網路辦理的比較沒有問題，因為二次登入時，系統會提醒更改。

1 兒科醫生電腦遭竊　3600孩童個資恐外洩

蘋果日報 2017.1.18

- 美國洛杉磯兒童醫院（Children's Hospital Los Angeles）表示去年他們一名兒科醫生放在車上的筆記型電腦被偷走，電腦內可能存有近3600名病童的個人病歷資料。本周在該院接受治療的數千名兒童的家人，將會接到通知信，知會他們孩子的個人資料可能已經外洩。
- 這部去年10月8日被偷走的筆電有密碼保護，但院方表示不確定它是否有加密，所以將會知會病童家人這件事。院方發言人貝尼特（Lorenzo Benet）表示，調查發現這部筆電失竊後未被用來上網，他們相信電腦內所有資料可能已經被刪除。
- 院方在聲明中提到：「另外，我們已經建立協定，（嫌犯）下次用這部裝置連上網路時，將會刪除裝置上的資料。」院方表示，洛杉磯兒童醫院和洛杉磯兒童醫院醫療集團是出於預防手段而通知病人。

Solution 1：資訊安全議題

BS 10012 Clause 8.2.11 安全議題

- 實行適當的技術上及組織上的安全措施和控制，確保個人資料受到保護，不會遭受未經授權或不合法的處理，並防止外部損失、破壞或損壞。

ISO 29100 Clause 5.11 資訊安全

- 堅持資訊安全原則， 意指下列事項：
  - 於主管機關許可下，於運作、功能及策略層級上以適宜之控制措施保護PII，以確保PII之完整性、機密性及可用性， 並於其整個生命週期中保護其免於受如未經授權之存取、破壞、使用、修改、揭露或損失的風險。
  - 實作控制措施，相稱於潛在後果之可能性及嚴重性、PII 之敏感性、可能受影響之PII 當事人數目， 以及其被持有之全景。
  - 對要求存取權限以執行其職責之個人，予以PII存取限制。限制上述個人之存取，僅限於其執行職責所需存取之PII。
  - 於持續之安全風險管理過程中，須定期審查及重新評鑑以管制控制措施。

Solution 1：資訊安全議題

ISO 27001 Standard

- Clause A.12.4.1 事件存錄
- Clause A.9.4.3 通行碼管理系統
- Clause A.14.1.1 資訊安全要求事項分析及規格
- Clause A.14.2.8 系統安全測試
- Clause A.14.2.9 系統驗收測試
- Clause A.16.1.3 通報資訊安全弱點
- Clause A.9.3.1 秘密鑑別資訊之使用
- Clause A.6.2.1 行動裝置政策
- Clause A.8.2.3 資產之處置
- Clause A.8.3.1 可移除式媒體之管理
- Clause A.10.1.1 使用密碼式控制措施之政策
- Clause A.11.1.3 保全之辦公室、房間及設施
- Clause A.11.1.2 實體進入控制措施
- Clause A.11.2.5 資產之攜出

2 拿抽獎個資推銷 濾水器業者觸法

自由時報 2016.10.29

- 參加抽獎填寫個人資料要小心！近來有濾水器業者以提供抽獎獎品給新開張的商家作為摸彩之用為由，取得民眾個資，並進行推銷，民眾不滿個資外洩，罵聲連連，新開張的商家名譽為此受損；屏東縣消保官盧仲炬表示，這種行為已涉及違反個資法，民眾可提出告訴。

- 萬丹鄉一家牛排店新開張，某濾水器業者主動表明要提供濾水器等摸彩品作為促銷，牛排店以為可以合作，不但花錢裝濾水器，還合作辦了摸彩活動，並請客戶留下姓名、電話、住址等個人資料，沒想到客戶的資料都被濾水器業者拿去使用，一一打電話推銷濾水器，優惠價也從三千二百元變為八千元，讓接到電話的民眾很生氣，紛紛向牛排店表達不滿。

- 牛排店發現事態嚴重趕緊補救，將所有摸彩券都從濾水器業者處拿回來，當眾錄影銷毀，並向所有客戶道歉，事後追查發現，這家販賣所謂磁能鹼性能量水的濾水器業者用這種方式促銷，已讓多家新開幕的商家名譽受損，生意受到影響，呼籲各商家及消費者多加注意，以免受害。

Solution 2-1：當事人告知

BS 10012 Clause 8.2.6 公平、合法與透明化的處理

- 確保個人資料被公平、合法與透明化的處理，並確認個人資料在開始處理前，均已清楚鑑別法律基礎。

ISO 29100 Clause 5.2 同意及選擇

- 堅持同意原則，意指下列事項：
  - 向PII當事人表明，以選擇是否允許處理其PII，除非PII當事人無不同意之自由，或所適用法律允許無須該自然人同意即可處理PII。PII當事人之選擇必須是自由提供、特定且基於充分理解。
  - 於取得同意前，通知PII當事人關於其在個人參與及存取原則下之權利。
  - 於取得同意前，向PII當事人提供以公開、透明及告知原則所表明之資訊。
  - 向PII當事人解釋給予或不予同意之涵義。

Solution 2-1：當事人告知

ISO 29100 Clause 5.8 公開、透明及告知

- PII處理之目的宜足夠詳盡， 以便使PII 當事人瞭解下列事項：
  - 所規定目的所要求之規定PII。
  - PII蒐集之所規定目的。
  - 所規定之處理(包括蒐集、溝通及儲存機制)。
  - 將存取PII及PII可轉移對象之授權自然人的型式。
  - 所規定之PII資料持有及廢棄要求。

Solution 2-2：蒐集、處理、利用特定目的

BS 10012 Clause 8.2.7 為具體指明合法的目的處理

- 確保組織僅為一個或以上具體指明的目的而取得個人資料，且不會以任何不符合此等目的的方式對個人資料做進一步的處理。
- Clause 8.2.7.1 處理的基礎
- Clause 8.2.7.4 資料分享

ISO 29100 Clause 5.3 目的適法性及規定

- 堅持目的適法性及規定原則， 意指下列事項：
  - 確保(各)目的均遵從適用之法律且依賴所允許的法律基礎。
  - 在為新目的而蒐集或第一次使用資訊之前，向 PII當事人傳達(各)目的。
  - 該規定宜使用清楚且適合環境之用語。

3 研究二二八 學者怨調資料遭個資法阻礙

自由時報 2017.2.25

- 二二八事件將屆滿70週年。臺灣師範大學臺灣史研究所教授范燕秋指出，進行加害者相關研究、調閱檔案時，檔案管理者常以個資法名義導致無法接觸到資料，如此何以達到真正轉型正義；中研院近史所研究員陳儀深則認為，此問題可透過尚未通過的「政治檔案法草案」與「促進轉型正義條例草案」來排除。

- 中央研究院臺灣史研究所與二二八事件紀念基金會合辦「紀念二二八事件七十週年」學術研討會，邀請多名學者發表相關研究。范燕秋發表「二二八事件後原住民身邊的情治人員」一文時，談及個人資料保護法對研究人員進行加害者研究及調閱資料時，造成阻礙。

- 范燕秋指出，加害者的研究室轉型正義中最重要的一部分，過去大家只知道二二八事件的被害者，卻對加害者面貌不清楚，但因碰觸到戰後的個人檔案資料，調閱過程中，檔案管理長常以個資法保護個人資料的名義，讓研究者無法接觸資料導致無法研究。

3 研究二二八 學者怨調資料遭個資法阻礙

- 范燕秋表示，此問題從個資法通過後便存在，國家檔案局及國史館於此情況下，會遮掩一些個資，不過會讓研究者看到大部分資料，但在調閱關係戰後各省級機關等更接近現代的資料，以進行研究加害者研究時，管理者會以個資法為由，使得無法申請調閱。

- 范燕秋指出，總統蔡英文宣誓要在最短時間內，進行轉型正義，尤其一定要釐清加害者部份的歷史責任，但若連檔案都看不到，無法讓研究者適度調閱檔案，以釐清相關人及理解當年加害的過程，如此無法讓受害者得到歷史了解與安慰，如此怎能做到轉型正義。

- 對此，陳儀深建議，可藉由尚未通過的「政治檔案法草案」及「促進轉型正義條例」來排除個資法及國家機密保護法所造成的問題，檔案一方面要公開，一方面卻又處及國家機密或個資，相互牴觸，但牽涉到人權及平反議題，不能因為此狀況就無法調閱。

Solution 3：資料分享基礎與處理方式

BS 10012 Clause 6.1.3 法源依據

- Clause 6.1.3.1 處理
  組織需經過辨識、定義與文件化其法源依據為處理所有的個人資料，法源依據可以由下選擇至少其中一項：
  - 自然人對其特定目的明確同意之必要；
  - 基於合約履行需要，自然人為契約或類契約的其中一方；
  - 組織基於履行法律義務之必要；
  - 基於保護自然人權益；
  - 當組織基於公共利益或政府授權要求時所履行之必要；
  - 基於資料控制者或第三方合法利益之必要，除自然人之基本權利與自由有利益衝突則另有規定(不適用於當公務機關執行公務時所必須實施之處理流程)；
  - 處理的其他法律規定請見本國法律。

Solution 3：資料分享基礎與處理方式

BS 10012 Clause 8.2.7.5 開放資料

- 當個人資料被發佈為「開放資料」的一部分時，個人資料應去識別化使該自然人無從識別，除非有公開個人資料的基礎。
- 當採取去識別化方式，應考慮可能用於重新識別自然人的所有合理手段。

Solution 3：資料分享基礎與處理方式

ISO 29100 Clause 5.6 利用、持有及揭露限制

- 堅持利用、持有及揭露限制原則，意指下列事項：
  - PII之利用、持有及揭露(包括移轉)限制於為履行特定、明確及合法目的所必要者。
  - 除非適用之法律明確要求不同的目的，否則將PII之利用限制於蒐集之前PII控制者所規定之目的。

ISO 29100 Clause 5.10 可歸責性

- PII之處理要承擔照管職責，並為其保護採用具體及實務的手段。堅持可歸責性原則，意指下列事項：
  - 當傳送PII至第三方時，確保第三方接收者一定會經由契約或其他如強制之內部政策(適用之法律可包含關於國際資料傳輸之額外要求)等手段， 提供相同等級之隱私保護。

4 元大人壽保戶資料外洩　遭詐騙集團掌握

TVBS 2017.3.1

- 台南地檢署偵辦電信詐騙案，發現元大人壽部分客戶資料，遭到詐騙集團掌握，檢方今天(1日)約談3名主管，以證人身分說明，訊後請回。元大人壽強調，他們也是受害者，願意配合調查，目前營運正常，保戶的保單權益，也不會受到影響。
- 知名的元大人壽，部分客戶資料疑似流入詐騙集團，台南地檢署在偵查電信詐騙案當中赫然發現，裡面有些個人資料都是元大人壽的保戶，台南地檢署2月24日，要求元大人壽協助調查，1日約談元大人壽，3位主管以證人身分說明，檢方訊問後請回，目前要追查，業者的客戶資料可能是哪個環節出問題，造成外洩。
- 元大人壽販賣的壽險產品相當多種類，客戶也不少，台南地檢署發現，詐騙集團掌握保戶名單，發現有異，不過元大人壽發聲明表示，案件疑似是有不法人士，透過不法管道取得保戶的相關資訊，強調元大人壽也是為受害者，目前案件還在偵辦中，元大人壽緊急發出聲明，就是希望保戶不要擔心，希望整起事件可以盡快釐清。

4 元大人壽保戶資料外洩　遭詐騙集團掌握

Solution 4：事件通報與處置

BS 10012 Clause 8.2.11.7 管理安全事件

- 個人資訊管理系統應實施下列措施：
  - 評估、管理和記錄所涉及個人資料安全事件，包括減緩任何安全事故所造成的損害的程序；
  - 任何有可能損害自然人的權利和自由的風險時，應在得知後72小時內通知主管機關此一安全事件。
  - 如果安全事件可能導致自然人權利和自由受到高風險影響，避免不當拖延、通知有顧慮的自然人。
  - 記錄每個安全事件，包括評估如何發生、採取的矯正行動，以及可以從中得到的教訓
  - 決定是否將安全事件通知主管機關(例如：金融監督管理委員會)；
  - 記錄任何核發的通知。

Solution 4：事件通報與處置

ISO 29100 Clause 5.10 可歸責性

- PII之處理要承擔照管職責，並為其保護採用具體及實務的手段。堅持可歸責性原則，意指下列事項：
  - 通知PII當事人關於可能對其造成實質損害之隱私權違反，以及採取之解決方法。
  - 於管轄權中之要求及依據風險等級，通知所有相關之隱私權利害相關者，隱私權違反事件。
  - 若發生隱私洩露，允許受侵害之PII當事人，存取適當及有效的制裁及/或補救。
  - 就自然人之隱私狀態難以或無法回復至事前狀態，考量其補償程序。
- 建立糾正程序係建立可歸責性之重要部分。糾正提供方法予PII 當事人，以使PII控制者為PII誤用負責。賠償係糾正之一種形式，涉及對受侵害之PII 當事人提供補償。此不僅對身分盜用、名譽損害或PII 誤用之情形係重要的，且對於修改或變更個別PII中造成錯誤亦是重要的。
- 當具備糾正過程時，PII當事人進入交易可能感覺更有信心，因為自然人關於結果所感知之風險被有效地減少。對於某些服務，糾正較易達成，而對於其他之糾正，較難具有對損失之量化及補償的能力。當基於透明及誠實原則時， 糾正效果最佳。所要求之糾正措施型式可依法律規定。

Solution 4：事件通報與處置

ISO 27001 Standard

- A.16.2.1 通報資訊安全事件
- A.16.1.4 對資訊安全事件之評鑑與決策
- A.16.1.5 對資訊安全事故之回應
- A.16.1.6 從資訊安全事故中學習
- A.16.1.7 證據之收集
- A.12.4.1 事件存錄
- A.12.4.2 日誌資訊之保護
- A.12.4.4 鐘訊同步
- 10.2 持續改善

5 南山人壽出包！　上百客戶個資外洩

蘋果日報 2016.8.30

- 南山人壽又出紕漏！南山工會指出，公司為了銷售，作業疏失大量洩漏個資，從上周四起，保戶陸續收到陌生人的保單資料，全台統計至昨天已有近百位保戶個資外洩。
- 南山工會昨天已向金管會檢舉，保險局官員也深皺眉頭，初步研判應是電腦失誤。
- 南山工會理事長嚴慶龍痛批，公司寄出的資料要保人與被保險不同人，為了銷售濫用個資，導致個資外洩，實在很離譜！外洩名單全台都有，可能會更多。
- 他說：「客戶大量反應封面是他的個資，內頁資料卻是不認識的人，造成客戶極度恐慌個資外洩。」法律遵循不遵守的公司，如同兆豐洗錢案，也是不遵守金管會法律遵循，內稽內控嚴重出問題。

5 南山人壽出包！　上百客戶個資外洩

- 工會指出，這批受害者多是民國82、84、89年滿期的保戶，公司為了行銷去撈一些舊客戶的資料，這些收到別人個資都是保單已經到期的保戶，公司想要繼續行銷寄資料，但打開內容卻赫然發現不是自己買的保單，而是別人的保單，也就是A收到B買的保單內容，包含保額與產品名稱等。除此之外，內頁還指定產品行銷人員的聯絡方式。
- 南山人壽表示，本公司近期對不需再繳保費的保戶，提供保單狀況一覽表，以利保戶了解保障內容；而在進行保單資料彙整時，部份資料檢核未盡完善，以致有些保戶資料受到影響，已陸續連絡保戶說明詳情並更新資料，保戶的保單權利完全不受影響。
- 南山人壽對於此內部疏失深表歉意，已第一時間更新資料，未來也將更謹慎檢視作業規範，以維護客戶權益。
- 工會表示，洩漏個資民事責任每人每一事件可求償500~2萬，同一件事最高可求償2億元。行政處罰最高可處5萬~50萬，並限期改正，未改正可按次處罰。

5 南山人壽出包！　上百客戶個資外洩

- 對此，金管會已接獲南山人壽工會檢舉保戶個資外洩情事，請南山人壽說明，公司可能涉及個資法，會依規定懲處，輕則限期改善，重則將處有期徒刑。且南山人壽7月初也因違反個資法，遭要求限期改善。
- 金管會傍晚表示，南山人壽涉及洩漏個資，是南山工會昨天向金管會檢舉，南山因為寄發客戶通知書、客戶繳費期滿，保單狀況的明細表，有100多筆保單客戶資料，在系統刪選上有疏漏，夾雜到其他同名的資料，因為工會都是業務員組織，客戶收到跟業務員說，因此才會透過工會檢舉。
- 金管會表示，後續會請南山人壽提供資料，如果違反個資法27條，會要求限期改善，必要時罰款2萬~20萬元，1次最高20萬元。
- 因為個資法在內稽內控辦法中，也有針對客戶資料和安全保護訂定規範，會檢視其內控作業有效性，若未建立或未執行 依此可處60~600萬罰款，將視情節輕重來衡量，也會請南山清查。

Solution 5：個人資料存取管制與程式變更

BS 10012 Clause 8.2.11.5 存取控制

- 在允許人員存取個人資料時，個人資訊管理系統應確保人員僅在職務上需要時才能存取個人資料。
- 如存取權是基於法律所賦予，個人資訊管理系統應確保人員清楚了解存取權僅為工作目的而賦予，且人員僅能為合法目的存取個人資料。
- 如處理的個人資料屬於高風險個人資料，個人資訊管理系統應確保存取權的控制措施能反映該個人資料的敏感度。
- 個人資訊管理系統應確保所有存取個人資料的行為是受到監督，且受到符合組織資訊安全風險評鑑。

ISO 29100 Clause 5.9 個人參與及存取

- PII控制者宜應用適當之控制措施，以確保PII 當事人僅限存取其本身而非其他PII當事人之PII，除非該存取之自然人在授權下行動，以代表不能行使其存取權利之PII當事人。適用之法律於某些情況下，可提供自然人對PII 存取、審查及反對處理之權利。

Solution 5：個人資料存取管制與程式變更

ISO 29100 Clause 5.11 資訊安全

- 堅持資訊安全原則，意指下列事項：
  - 於主管機關許可下，於運作、功能及策略層級上以適宜之控制措施保護PII，以確保PII之完整性、機密性及可用性，並於其整個生命週期中保護其免於受如未經授權之存取、破壞、使用、修改、揭露或損失的風險。
  - 選擇PII處理者，其對PII處理之關於組織、實體及技術的控制措施提供充分保證，並確保遵循此等控制措施。
  - 對要求存取權限以執行其職責之個人，予以 PII存取限制。限制上述個人之存取， 僅限於其執行職責所需存取之PII。
  - 於持續之安全風險管理過程中，須定期審查及重新評鑑以管制控制措施。

Solution 5：事件通報與處置

ISO 27001 Standard

- A.14.2.2 系統變更控制程序
- A.14.2.5 保全開發環境
- A.14.2.8 系統安全測試
- A.14.2.9 系統驗收測試
- A.14.3.1 測試資料保護
- A.15.1.2 於供應者協議中闡明安全性
- A.15.2.1 供應者服務之監視及審查

ISO 22301 Clause 8.4.2 事件回應架構

- 組織應建立，實施與維持程序與一個管理架構，藉由使用有必要職責，授權與勝任力的人員來回應一個中斷事件以管理一個事件。
- 此回應架構應：
  - d. 針對回應的啟動，運作，協調與溝通建立其流程與程序
- 組織應以生命安全為第一優先以及諮詢相關利害關係者來決定是否對外溝通有關其重大風險與衝擊，並且書面化其決定。假如決定是要溝通則組織應針對外部溝通，警報與警示建立與實施程序，當適當時包括媒體溝通。

6 幫客人換電腦硬碟　員工偷看她資料夾A片

蘋果日報 2016.9.26

- 店家幫客人換電腦硬碟，竟私自打開資料夾偷看A片。
- 今日出版的《自由時報》報導，陳姓女子買新電腦時，將舊電腦交給店家換裝硬碟，強調內有隱私，請勿開啟，陳女隔天前往取機，開啟電腦，發現最近使用資料夾內，曾遭開啟「重要資料」的資料夾，內有個人私密照片、私生活紀錄、身分證、健保卡、信用卡照片、電子郵件帳號密碼、網路銀行帳號密碼等資料，另還有原儲存舊硬碟內成人影片的瀏覽紀錄。
- 陳女怒告店家與員工須連帶賠償。電腦公司稱，當天店內人員交接，擔心檔案無法正常開啟使用，為測試才開啟電腦內數個檔案，誤開陳女個人資料，但並未看到檔案內容，無侵害資訊隱私權。法官認為，店家未盡監督責任，且員工不法侵害陳女資訊隱私權，均應負過失侵權損害賠償責任，判員工與店家連帶賠償6萬元。

Solution 6：委外廠商的監督與管理

BS 10012 Clause 8.2.11.10 委外處理個人資料

- 如資訊是委外其他組織處理，個人資訊管理系統應確保下列事項：
  - 僅選擇可以提供技術、實體和組織安全措施的組織作為資料處理者，以符合組織要求代表組織處理所有個人資料；
  - 在與另一個組織締結合約前，進行適當安全性的評估，作為盡責調查(D.D)的行動之一，且如果因為將處理的個人資料之本質或處理的特殊狀況所需要，組織在締結合約之前應對其作為資料處理者的組織的安全措施安排進行稽核；
  - 對擔任資料處理者的組織進行盡職調查；
  - 一旦挑選了作為資料處理者的組織時，組織應簽訂具有拘束力的書面協議或契約。

Solution 6：委外廠商的監督與管理

ISO 27001 Standard

- A.8.2.3 資產之處置
- A.8.3.1 可移除式媒體之管理
- A.8.3.2 媒體之汰除
- A.10.1.1使用密碼式控制措施之政策
- A.11.2.5 資產之攜出
- A.11.2.6 廠外設備及資產之安全
- A.15.2.1 供應者服務之監視及審查

7 瓜國戶政搞烏龍 男子身分證誤植妻個資

中央通訊社 2016.10.25

- 超離譜！中美洲瓜地馬拉戶政單位將一男性國民的身分證上的個人資料誤植為其妻子的個資，但是該男子目不識丁，渾然不知身分證資料有誤，直至近日才被告知並再度申請補發，但戶政人員要求他繳費換發新證，令他頗不以為然。
- 據瓜地馬拉「自由新聞報」報導，此起令人不可思議的身分證個資誤植事件發生於瓜國北部上維拉帕斯省潘索斯市國民身分登記處。市民耶夫拉印·喬科於2013年2月9日辦理換發身分證，由於他不識字，故未發覺身分證上的個資被戶政人員誤植為其妻子波琳·喬科·莫蘭的個資。
- 報導說，近日喬科向當地一公立機構出示身分證辦理某些必要手續時，承辦人員告知他身分證個資遭誤植，於是他再次到潘索斯市國民身分登記處申請更正個資，但是該登記處不承認作業疏失並要求他繳交規費才能更正，令他相當憤慨。
- 潘索斯市國民身分登記員嬌婉娜·喬凡諾尼對媒體表示，前幾年也曾發生國民身分證資料錯誤的情況，但是將男性的個人資料誤植為女性實在是不可思議，登記處將重新檢視輸入系統的所有個資以避免再度發生類似張冠李戴事件。

Solution 7：維護個人資料正確

BS 10012 Clause 8.2.9 正確且最新

- 個人資訊管理系統應確保被處理之個人資料維持完整和正確性。
- 個人資訊管理系統應確保讓自然人能夠質疑其個人資料之正確性，並在需要時要求更正其個人資料。當個人資料為不正確且無法更正時，例如與歷史紀錄，個人資訊管理系統應記錄不正確處，並適當提供正確的個人資料。
- 個人資訊管理系統應具有已核准及文件化過程來檢查個人所聲稱的不正確資訊是否屬實。經過檢查後，若聲稱的不正確處是錯誤，而實際上資料是正確的，個人資訊管理系統應保留適當的證據。
- 個人資訊管理系統應確保人員被告知正確記錄個人資料的重要性，以及僅使用最新的個人資料來做出與自然人有關的重要決定。
- 個人資訊管理系統應處理以下事項：
  - 當組織分享不正確或過時的個人資料給任何第三方時，應告知該第三方此等資訊不應被用來做出與該自然人有關的決策；
  - 在需要時將任何更正的個人資料分享給第三方。

Solution 7：維護個人資料正確

ISO 29100 Clause 5.7 準確性及品質

- 堅持準確性及品質原則，意指下列事項：
  - 確保所處理之PII為準確、完整、最新、適度的，且與使用目的相關。
  - 於處理前，確保由非PII當事人之來源所蒐集的PII 之可靠性。
  - 變更PII前，經由適當方法查證PII 當事人聲明之有效性及正確性(以確保該等變更經適當授權)。
  - 建立PII蒐集程序，以協助確保PII之準確性及品質。
  - 建立控制機制，以定期核對所蒐集及儲存之PII的準確性及品質。
- 於資料可能被用以對自然人授予或拒絕重大利益之情形下，或不準確之資料可能在其他方面對自然人造成傷害時，本原則特別重要。

Solution 7：維護個人資料正確

ISO 29100 Clause 5.7 準確性及品質

- 堅持準確性及品質原則，意指下列事項：
  - 確保所處理之PII為準確、完整、最新、適度的，且與使用目的相關。
  - 於處理前，確保由非PII當事人之來源所蒐集的PII 之可靠性。
  - 變更PII前，經由適當方法查證PII 當事人聲明之有效性及正確性(以確保該等變更經適當授權)。
  - 建立PII蒐集程序，以協助確保PII之準確性及品質。
  - 建立控制機制，以定期核對所蒐集及儲存之PII的準確性及品質。
- 於資料可能被用以對自然人授予或拒絕重大利益之情形下，或不準確之資料可能在其他方面對自然人造成傷害時，本原則特別重要。

ISO 27001 Standard：A.8.2.3 資產之處置、A.14.1.1 資訊安全要求事項分析及規格
A.14.1.3 保護應用服務交易

bsi.

...making excellence a habit.™