bsi.

# 個人資料保護
# 認知宣導與案例分享

## 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

## 課程目的

- 個人資料保護法於2012年10月1日正式實施，並於2016年3月15日實施修法後之新版個人資料保護法，鑑於個人資料安全防護及當事人權益保障越來越受到民眾的重視，教育機構在歷年來取得大量之個人資料，除了使目的得以達成外，如何有效的符合法律規範、保護當事人人格權，已成為實現善良管理責任及兼顧社會安定重要議題。

- 本課程的目的便是希望透過課程的介紹，是希望除了能從立法精神看我國個人資料保護法對取得個人資料之機構應有之注意義務與要求外，並進一步從管理方向思考建立符合國際標準之管理制度以符合個人資料保護法之要求。

## 課程大綱

- 前言
- 法制先進國家個人資料保護及隱私權法演進介紹
- 個人資料保護法與施行細則重點摘要
- 從當事人角度看組織應有的個人資料保護
- Q&A

# 前言

bsi.

## BCI BSI 2017 Horizon Scan Report

2017 BCI 地平線掃描

726

79

### 前10大威脅(Threats)

1st 網路攻擊 Cyber attack

2nd 資料外洩 Data breach

3rd 無預期的資訊與通訊中斷 Unplanned IT and telecom outages

4th 安全事故 Security incident

5th 惡劣氣候 Adverse weather

6th 公共服務中斷 Interruption to utility supply

7th 恐怖主義行動 Act of terrorism

8th 供應鏈中斷 Supply chain disruption

9th 人才／關鍵技術的可用性 Availability of talents/key skills

10th 新頒布之法令或法規 New laws or regulations

# BCI BSI 2017 Horizon Scan Report

## 前10大衝擊(Disruptions)

1st 無預期的資訊與通訊中斷 Unplanned IT and telecom outages

2nd 惡劣氣候 Adverse weather

3rd 公共服務中斷 Interruption to utility supply

4th 網路攻擊 Cyber attack

5th 安全事故 Security incident

6th 運輸網路中斷 Transport network disruption

7th 人才／關鍵技術的可用性 Availability of talents/key skills

8th 供應鏈中斷 Supply chain disruption

9th 資料外洩 Data breach

10th 新頒布之法令規法規 New laws or regulations

# BCI BSI 2017 Horizon Scan Report

## 前10大趨勢(Trends)

1st 使用互聯網進行惡意攻擊 Use of internet for malicious attacks

2nd 社群媒體的影響 Influence of social media

3rd 流失重要員工 Loss of key employee

4th 新法規和更高級的監管審查 New regulations and increased regulatory scrutiny

5th 互聯網相關服務的普及和高度採用 Prevalence and high adoption of internet dependent services

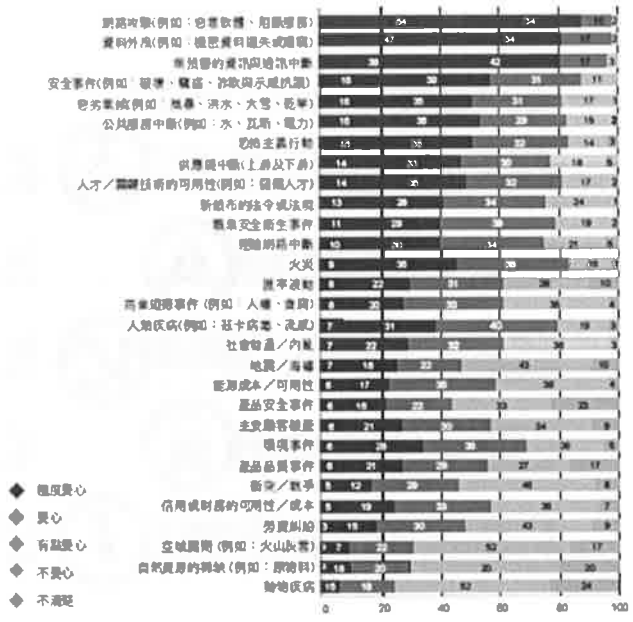
6th 政局變化 Political change

7th 供應鏈複雜度提升 Increasing supply chain complexity

8th 潛在的全球疫病爆發 Potential emergence of a global pandemic

9th 消費者態度與行為改變 Changing consumer attitudes and behaviour

10th 經濟成長趨緩以及對於投資的影響 Slow economic growth and its impact on investment



# 歐洲議會：要用個資進行大數據應用 需先去識別

DIGITIMES 2017.03.23

- 隨著物聯網裝置數量不斷增加，各種大數據(Big Data)應用也愈來愈熱，許多公司都看準大數據所帶來的商機，但如何在利用資料同時保護個人隱私權，也是各界應積極重視的議題。
- 歐洲議會近日就針對大數據應如何使用個資，提出明確立場。
- 據Bloomberg BNA報導，歐洲議會於14日提出，公司在大數據應用中使用個人資訊之前，必須先對個人資訊進行去識別(de-identify) 以保護隱私。
- 報導指出，在不具約束力的決議中，議會表示歐盟的隱私監管人員會針對匿名化(anonymization)發佈指導(guidance)，以確保在大數據應用中，隱私權不會受到侵害，此外，決議也提出，大數據每年成長4成，應該鼓勵研究要確保用在匿名化與加密個人資料的技術能夠提供強健的保護。

# 歐洲議會：要用個資進行大數據應用 需先去識別

- 此外，葡萄牙中間左派的立法者Ana Gomes，同時是決議的作者，在投票前於議會中表示，大數據應用中運算法的使用可能對於人們的私生活帶來實質的影響；而歐盟司法專員(EU Justice Commissioner) Vera Jourova也在前一日的辯論上指出，這樣的決議來的時機剛剛好，因為歐盟所推出新的隱私體制「一般資料保護法」(General Data Protection Regulation)，以及有關資訊網絡安全與線上隱私(e-privacy)等其他歐盟法規，將會在接下來的數年內生效，並為大數據相關的隱私保護提供架構。

# 1 垃圾郵件集團意外曝光近14億筆個人資料

iThome 2017.03.07

- MacKeeper研究人員Chris Vickery近日指出，披著合法行銷公司外衣的River City Media（RCM）因資料庫配置不當，讓伺服器上的大量資訊曝光，曝露出該公司所蒐集的13.7億筆個人資料，以及不為人知、違法的郵件發送手法。
- 這是因為RCM未能妥善地配置伺服器上的檔案傳輸與同步機制rsync，而使得伺服器上的資料門戶大開，而且已曝光超過一個月。
- 在RCM伺服器上發現的13.7億筆個人資料包含了使用者的電子郵件帳號、全名、IP位址，還有許多的實體地址。Vickery相信這批資料來自不同組織、以不同的手法所蒐集，例如藉由免費郵件、信用檢查、教育機會等行銷郵件引誘使用者分享個人資訊，經查證後，他認為這批資料是真實的。
- 除了使用者個資外，Vickery還發現該伺服器上擁有RCM的財務文件、聊天紀錄與其他備份，顯示該公司透過攻擊手法發送大量垃圾郵件。

# 1 垃圾郵件集團意外曝光近14億筆個人資料

- RCM採用的是可造成分散式阻斷服務的慢速攻擊（Slowloris）手法，漸近式地利用自家的2199個IP建立與電子郵件伺服器的持續連線，在伺服器察覺負載過重並切斷連線之前，一口氣利用所有的通道傳遞大量的郵件。所攻擊的對象包含Gmail、Hotmail及AOL等。
- 由於RCM將自己包裝成合法的行銷公司，因此所發送的垃圾郵件涉及不少知名品牌，像是Nike、Victoria's Secret、Yankee Candle與AT&T。
- 執法機構已在接到MacKeeper的通知後展開調查，而RCM的部份客戶在得知此事後也已中止與該公司的往來，預期RCM很快就會從市場上消失。

# 2 中國強制無人機實名制 登記個人資料才能購買

聯合新聞網 2017.05.17

- 由於民用無人機違規飛行干擾各大城市機場的航班起降，中國民航管理部門宣布自2017 年 6 月 1日起，消費者購買重量在 250 公克以上的無人機都必須進行實名登記和註冊，同時無人機登記註冊資料將與無人機運作平台資料互通。嚴格的監管制度有可能會對無人機的銷售帶來衝擊。
- 小型無人機進入消費市場後，在技術和市場需求的推動下，市場規模爆發式成長，無人機給用戶帶來了全新的空拍體驗，但無人機違規飛行給城市管理帶來的挑戰也日趨突顯。
- 近期中國多個城市的機場遇到無人機違規飛行干擾航班起降事件。沒有在監管平台登記和註冊的飛行器，出現在民用機場淨空保護區內時，為避免發生相撞事故，航班不得不改變航路，同時影響其他航班起降。
- 在 2017 年 4 月 14 日至 18 日成都機場連續發生 3 起無人機干擾航班起降的事件，同時公安部門開始介入調查，但無人機擾飛卻越來越嚴重，4 月 21 日至 30 日成都機場再次連續發生無人機擾飛事件，導致多航班轉降其他機場或返航。

# 2 中國強制無人機實名制 登記個人資料才能購買

- 隨著無人機越來越普及，購買和使用無人機對普通消費者都不難，目前中國大約有2 萬台消費級無人機，但持有無人機使用認證的用戶僅 1 萬人，超過五成無人機都是違規飛行。據知情人士透露，推行無人機實名制已勢在必行，消費者購買無人機需要出示相關部門認證的資料登記證明和飛行許可證，便於政府管理和監控。
- 中國民航局表示民用無人機登記註冊系統的開發已經完成，將在 2017 年 5 月 18 日上線運作，自 2017 年 6 月 1 日起對 250 公克以上的無人機實施登記註冊，同時建立無人機登記資料共享和查詢制度，與無人機運作平台即時連線。目前市場上較受歡迎的大疆無人機屬於實名登記範圍。
- 民用無人機實施實名制管理並非首次出現，美國在 2015 年 12 月開始對小型無人機實行實名註冊制度，確保能追蹤到違規飛行的無人機使用者，保證低空域安全。重量在 250 公克到 25 公斤內的無人機都必須註冊，消費者需要提供姓名、電子郵件和住家地址，註冊有效期為 3 年，每次註冊費用為 5 美元。 2016 年 6 月美國聯邦航空局又頒布新規，要求所有 25 公斤內的無人機在飛行時，都必須在操控者的視線範圍內，距離機場至少 8 公里，遇到飛機必須避讓，操控者必須持有遙控飛行證書。 Google、Amazon、Verizon 等公司正與 NASA 合作開發全球首個無人機交通控制系統，防止無人機發生空中交通事故。

## 3 高師大獎懲系統更新出錯 學生意圖性侵資料曝光

自由時報 2017.05.18

- 高雄師範大學的網路學生獎懲查詢系統，昨晚進行系統功能更新時，因資訊人員的疏失，導致全校 6000 多名學生若以個人帳號密碼登入查詢獎懲紀錄時，都出現一名男同學個人獎懲紀錄，內容顯示該這名學生曾「意圖性侵害、情節嚴重」遭記小過及申誡處分，但後來都已功過相抵。
- 這起個人資料外洩意外，昨晚 9 點多，有學生在網路反映此事，校方今凌晨3時許得知，已立即更正，高師大學務長李金鴦表示，今上午緊急聯繫這名男學生，她與校長都向男學生致歉，希望學生能諒解。
- 有學生將訊息貼上「靠北高師大」臉書專頁，要大家快去看獎懲記錄，並表示「莫名其妙多了小過，事由還寫意圖性侵，根本是危害我們，要是在求職或考正式老師的時候，對方問為何會有意圖性侵，我們要如何解釋？」也有人回應「這應該是機密件吧？這樣全校都知道有某學生意圖性侵了」。

## 4 破獲全台最大個資販賣案 身分證、電話地址全都露

聯合新聞網 2017.05.11

- 調查局破獲全台最大個資販賣案！調查局日前查獲以梁姓、蘇姓主嫌為首的軟體販賣集團，該集團主打房仲業者，開發出可「客戶開發搜尋系統 V5.0 專業版」，只要購買軟體後，房仲可依靠資料比對搜出土地所有者，進而搶賺業績，但事實上該軟體卻已內建民眾個資達 200GB 以上，只需輸入姓名，身分證字號、地址、電話都無所遁形，警方目前將涉案的 62 人約談到案，詢後依個人資料保護法移送法辦。
- 調查局航業處台中站副主任吳幸燦表示，調查局在今年三月接獲民眾報案，有不法集團涉嫌販售個資，於是組成專案小組偵查，發現梁姓、蘇姓男子為首的犯罪集團，從 105 年開始，以個資資料庫為基礎，撰寫「客戶開發搜尋系統 V5.0 專業版」系統，後，由底下人員以 LINE 代號「房仲開發利器」、「房仲省時尋人系統」，在全國針對房仲、地產開發商等特定業者販售該套軟體，每套以 15 至 20 萬元售出，提供業者針對特定標的，可輕易查出地主資料及聯絡方式，進而搶賺仲介利潤。

# 4 破獲全台最大個資販賣案 身分證、電話地址全都露

- 據了解，該軟體開發出可破解地政局用於阻擋機器人的圖形辨識系統，可在短時間在地政局查出大量土地資訊，雖然地政局的資料並不完全，但資料庫擁有 200GB 以上的個人資料，可供查詢對象交叉比對篩選，尤其查詢者只需要輸入姓名，系統就可查到身分證字號、電話、生日、地址等資料，讓民眾的個人資料早已「看光光」，雖然可能資料有些許重複，但交叉比對之下，仍無所遁形。
- 吳幸燦說，梁姓、蘇姓主嫌以前曾是房仲同事，利用來源不明的程式與資料庫撰寫軟體販賣業者圖利，雖然目前僅有查獲房仲程式版，但警方憂心不法集團早就將個資販賣給討債公司、是詐騙集團，讓全台民眾的個資都不安全，目前正循線追查個資的來源及已流出市面上的 300 多份軟體。

# 5 送錯樓！女控宅配出包　個人醫療資料外洩

TVBS 2017.04.08

- 台北市一名林小姐控訴，送貨員把包裹送錯到別層樓，鄰居也沒仔細看就簽收了，打開發現裡頭有健保卡和就診資料，讓林小姐非常氣憤，認為隱私曝光，向宅配公司求償，業者坦承疏失，未來將加強送貨員 SOP 落實。
- 投訴人林小姐：「這是我的包裹，因為被送錯資料被鄰居拆封。」
- 手中拿著包裹，林小姐越講越氣，指控送貨員出包，害她個資差點外洩。去年聖誕節，朋友把包裹寄到林小姐一樓住處，裡頭有健保卡、就醫資料光碟和委託書，送貨員看錯樓層，把一樓包裹錯送到二樓，鄰居以為是小孩網購物品直接簽收，送貨員也沒檢查，直到鄰居打開才驚覺，東西送錯了。
- 投訴人林小姐：「鄰居不小心拆封了，沒有注意到收件的人住址不是他們家的，姓名也不是他們家的，裡面有我的一些就醫資料，已經有侵犯到我的隱私。」
- 事後林小姐向宅配公司求償，業者回應，雙方有開調節會，未來將加強送貨員 SOP 落實，不過一般民眾網購，常會請家人、朋友代收，如果是隱私物也能這麼做。

# 6 無良空軍上尉樂透輸百萬　盜賣400官兵個資抵債

蘋果日報 2017.05.09

- 空軍新竹基地張姓上尉參謀官因愛玩樂透彩，輸了上百萬元，向 12 家地下錢莊借貸 100 萬元債務，因無力償債，竟將基地內 400 筆個人資料，在基地前交付給錢莊業者做抵債，並獲得 3000 元報酬。事後錢莊業者打電話到基地內部嗆聲「我手中握有你們基地官兵的個資！叫張男趕快還錢！」，基地政戰保防官進行調查，才揭發本案，並函由新竹檢方偵查，上周檢方依違反個人資料保護法起訴張男。
- 檢方調查，空軍第 499 聯隊部上尉電子戰張姓參謀官是負責資訊、電戰業務，業務涵蓋通信、電子、資安等，甚至官兵手機申請。因張玩樂透彩輸了上百萬元，去年十月向錢莊借錢，高達百萬元，只是他無力償債，去年 11 月間，又向綽號小陳的男子借 5 萬元，被要求簽下 9 萬元本票，但張男周轉不靈，無法支付利息。
- 陳男得知張男是空軍上尉，且知道他的業務負責基地同袍的通訊個資，竟要求張男交出聯隊官兵姓名與電話資料，越多越好，若有辦法交出，他就以名單作為抵押，利息部份可先緩還。

# 6 無良空軍上尉樂透輸百萬　盜賣400官兵個資抵債

- 由於張男無力付利息，小陳竟打電話到空軍新竹基地催債，當時張男不在，由保防官接聽，小陳向保防官嗆說手中握有基地官兵名單資料，要張男趕快還錢，保防官大驚，小陳甚至用 LINE 上傳用手機拍下的官兵名單照片，空軍基地警覺事情大條，將全案移送檢方偵辦。
- 張姓上尉向檢方坦承，因周轉不靈無法支付利息，才列印官兵姓名電話，在營區斜對面的加油站給人。張男說他當時只是隨機列印的，不知道洩漏出去的名單當中有誰，想要事後防堵，也沒有辦法。空軍總部得知此事後，今年 1 月中旬將張姓上尉調往台東基地服務。
- 新竹地檢署上週將全案依違反個人資料保護法起訴，由於張男是公務員利用職務上機會涉犯個人資料保護法之罪，依法需加重其刑至二分之一。張男也已被軍方革職 。

# 法制先進國家
# 個人資料保護
# 及隱私權法演進介紹

bsi.

## OECD 隱私保護與個人資料跨境傳輸指引

- 源起：
  - 新興科技下面對個人資料跨境傳輸下的挑戰，例如：非法儲存個人資料、不正確使用個人資料、個人資料不當揭露等
  - 作為已有個人資料保護成文法國家或尚未立法國家擬定參考
- 共識：
  - 不同國家法律要求下，對個人隱私與資訊流通的視為基本價值
  - 自動化跨境傳輸與處理個人資料時所衍生的規範與要求
  - 顧及個人資料跨境傳輸時的經濟與社會發展
  - 立法時對於個人資料跨境傳輸的阻礙與限制
- 建議會員國：
  - 參考本指引作為立法保護隱私的依據並避免法律上訂定跨境傳輸不當的障礙
  - 參考附錄作為合作建置基礎並進快建立具體合作程序

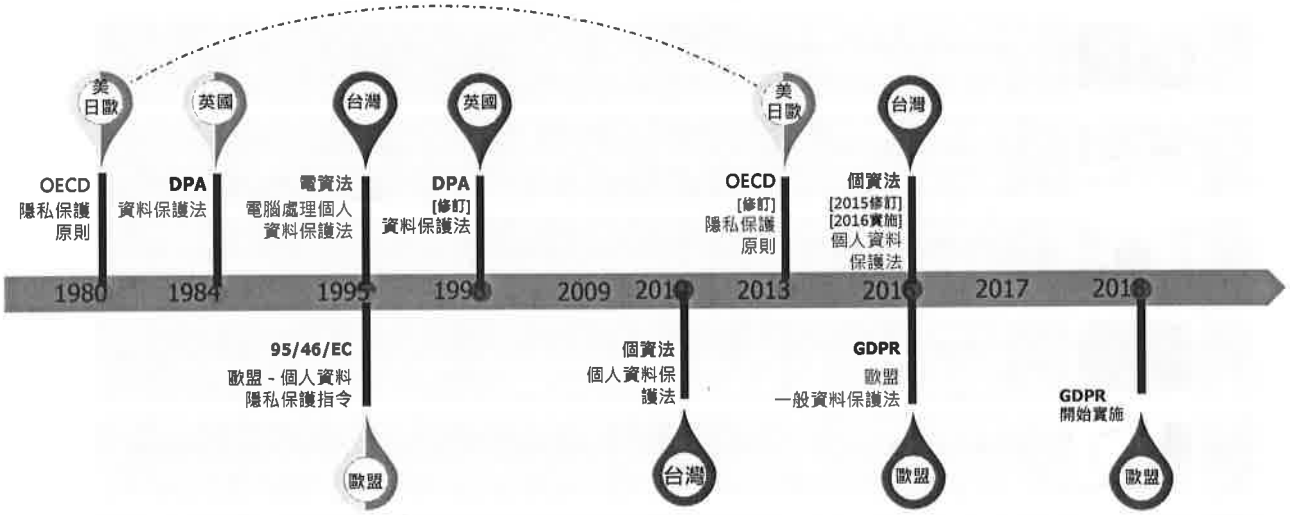
# OECD 隱私保護與個人資料跨境傳輸指引

- Part 2 基本原則 (第7條至第14條)：
  - Collection Limitation Principle 蒐集限制原則
    §7. 個人資料的蒐集應有一定的限制，應基於合法與公平的方式，在適當情形下令資料主體知悉或同意。
  - Data Quality Principle 資料品質原則
    §8. 個人資料應與使用目的相關，且在該目的必要範圍內，個人資料應保持正確、完整並及時更新。
  - Purpose Specification Principle 目的特定原則
    §9. 蒐集個人資料的目的應具體，不晚於資料蒐集時；其後個人資料的使用，應以達成上述特定目的為限，不會用於不相容的目的上
  - Use Limitation Principle 利用限制原則
    §10. 個人資料不應被揭露，僅能用於第9條所定義之目的，除非：
    - 經資料主體同意，或；
    - 基於法律明文要求

# OECD 隱私保護與個人資料跨境傳輸指引

- Part 2 基本原則 (第7條至第14條)：
  - Security Safeguards Principle 安全原則
    §11 個人資料應被合理安全保護以避免遺失或未經授權存取、使用、修改或揭露資料等風險。
  - Openness Principle 公開原則
    §12 應有個人資料的發展與運用的公開政策，應建立合理管道以確認個人資料的存在與否及性質、使用目的，以及資料管理者的身分及地址
  - Individual Participation Principle 個人參與原則
    §13 當事人應具有下列權利：
    - 向資料管理者確認其是否擁有關於資料主體的資料
    - 於合理期限、合理金額、方式，以及可以理解形式，取得相關資料；
    - 如果前述兩項請求被拒絕時，應獲知理由，並有救濟管道；
    - 對個人的資料提出異議，並請求刪除、更正、補充及修改相關資料。
  - Accountability Principle 課責原則
    §14 資料管理者違反上述個人資料保護原則時，應負擔一定責任。

# 國際間個人資料保護法制關連說明




# 歐盟 GDPR 簡介

## Key Definitions~ Article 4

- "Personal data" includes: online identifiers (IP address, cookies)
- "Pseudonymised" data (e.g. key-coded or hashed data)
- "Sensitive personal data": includes genetic or biometric data

## Substantive scope~ Article 28 to 30

- Under Directive, only controllers.
- Processors now in scope

## Territorial Scope~ Article 3

- Controllers and processors not based in the EU who sell to individuals who are in the EU.
- Or who monitor individuals in the EU

# GDPR- 資料保護六大原則~ Article 5

**Lawful, fair and transparent**

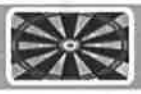
processed lawfully, under a specific justification

**Purpose limitation**

collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

**Data minimisation**

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;



**Accuracy**

accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay;

**Storage limitation**

kept in identifing form for a time no longer than justified by the purposes for whichthe data is collected

**Integrity & Confidentiality**

processed in a manner that ensures appropriate security of the personal data;

# GDPR- 資料控制者與資料處理者應有之責任與義務

## Privacy by Design and by Default~ Article 25

- Privacy needs to be built into any new system, business processes, technologies, operations and information architecture from the outset
- **ENGINEERING IMPACT:**
  - The design of programs, information and communications technologies, and systems, should by default collect the minimum amount of information necessary.
  - Individual's personal information should not be shared widely by default.
  - Privacy must be "baked-in" to any product developments

# GDPR- 資料控制者與資料處理者應有之責任與義務

Privacy Impact Assessments~ Article 35 & 36

- If processing is likely to result in high-risk to individuals (particularly when using new tech & taking into account nature, scope, context and purposes of processing), prior to processing.
- In particular, processing based on automated processing (incl. profiling).
- Large-scale processing of sensitive personal data.
- **ENGINEERING IMPACT**:
  - Analysis / Describe: What data is being collected, why, the "legal basis".
  - Assesses: Necessity and proportionality of processing operations and risks to individuals' rights
  - Confirms measures to address the risks
  - If PIA confirms processing is 'high-risk', controller must consult with the regulator before processing begins





# GDPR- 資料控制者與資料處理者應有之責任與義務

Data Protection Officers~ Article 37 to 39

- GDPR = requirement for controllers and processors
- Threshold for appointment:
  - public authorities
  - core activity = 'large scale' regular and systematic monitoring of individuals
  - core activity = 'large scale' processing of sensitive data
- Can be employee or outsourced DPO, must be a privacy expert
- Group of undertakings may have a single DPO
- DPO to be involved in all personal data issues, has board level access, adequate resource, 'impartial', no conflict of interest or dismissed for performing DPO tasks

# GDPR- 當事人權利

## Now

Individuals have the following rights:

- Right to be informed about the collection/processing of their personal data no later than the time of collection.
- Right to access and obtain a copy of their data.
- Right to amend, correct /update and delete their information.
- Right to object to use of their information.
- Right not to be subject to fully automated decisions.
- (Under case law) right to be forgotten.

## GDPR

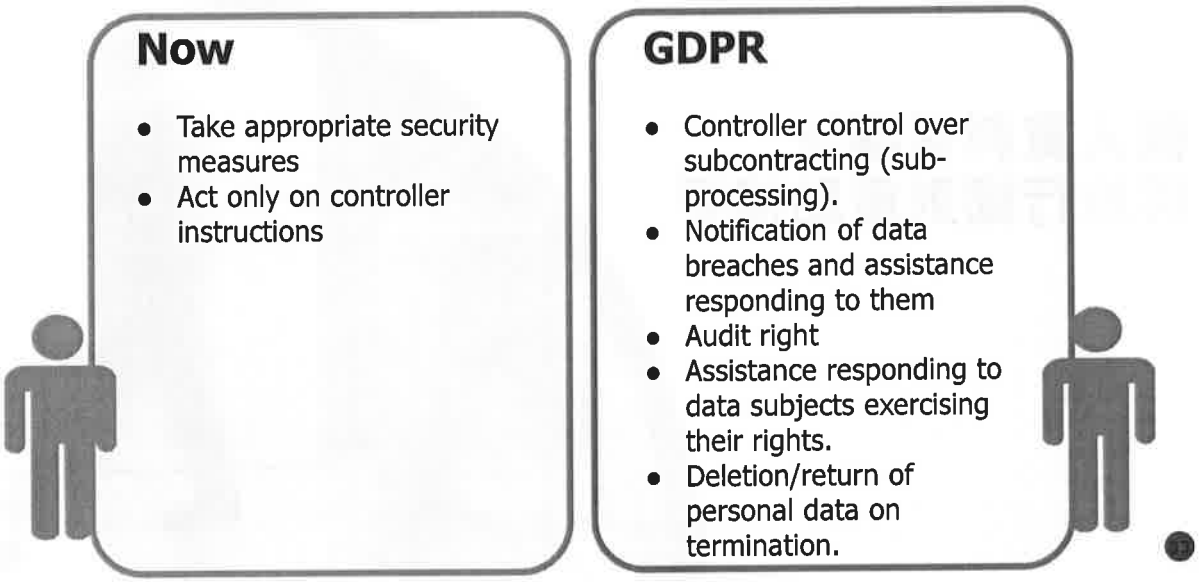
GDPR maintains existing and expands or introduces new rights:

- Article 17
  Right to erasure (and right to be forgotten).
- Article 18
  Right to restrict the processing of personal data.
- Article 20
  Right to the portability of data.
- Article 22
  Automated individual decision-making, including profiling

# GDPR- 個資外洩事故通知~ Article 33 & 34

1. Controllers must notify **regulator** within **72 hours**, unless unlikely to result in a risk for data subjects
2. Controllers must notify **individuals**, if breach is likely to result in a high risk for data subjects.
3. Processors must inform **controllers** of a data breach **"without undue delay"**

## GDPR- 委外管理責任




## GDPR- 行政處罰~ Article 83

- Maximum fine for both controllers and processors is up to 2% (or €10m) or 4% (or €20m) of global annual turnover
- Maximum fine depends on which provision are being infringed

| 2% (or €10m) | | 4% (or €20m) | |
|---|---|---|---|
| Data protection by design/default | Identifying a data subject | Principles for processing including fairness and security | Lawful processing conditions |
| Children's consent | Joint controllers | Consent | Transfers |
| Designating a representative | Data Impact Assessments | Information provided to data subject | Processing sensitive data |
| Cooperation with SA | Consultation with SA | Right to rectification | Right to access |
| Appointing DPO | Processing records | Right to erasure | Right to restriction |
| Breach notification | Processor agreements | Contrary to limitation | |

# 個人資料保護法
# 與施行細則重點摘要

bsi.

## 蒐集、處理或利用個資的特定目的

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。

**定義**

- 蒐集資料時所指定的使用目的：目的特定原則

**功能**

- 結合「使用限制 / 目的拘束 / 目的限縮原則」原則：指個人資料的處理、利用，除有例外情形，應符合原先蒐集時所指定的目的。
  禁止不特定或無特定目的的資料蒐集。

## 蒐集、處理或利用個資的特定目的

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實施辦法

第六條

- 學校、機構應確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查所保有之個人資料現況。
- 學校、機構經定期檢視，發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理或利用等適當之處置。

## 非公務機關蒐集、處理個資的合法手段

第十九條

- 非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. 法律明文規定。
  - 二. 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。
  - 三. 當事人自行公開或其他已合法公開之個人資料。
  - 四. 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。
  - 五. 經當事人同意。
  - 六. 為增進公共利益所必要。
  - 七. 個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。
  - 八. 對當事人權益無侵害。
- 蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，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。

## 非公務機關利用個資的合法手段

第二十條

- 非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，應於蒐集之特定目的必要範圍內為之。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. 經當事人同意。
  - 七. 有利於當事人權益。
- 非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。
- 非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。

## 非公務機關利用個資的合法手段

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實施辦法

第十條

- 學校、機構利用個人資料為宣傳、推廣或行銷時，應明確告知當事人其所屬學校、機構立案名稱及個人資料來源。
- 學校、機構於首次利用個人資料為宣傳、推廣或行銷時，應提供當事人表示拒絕接受宣傳、推廣或行銷之方式，並支付所需費用；當事人表示拒絕宣傳、推廣或行銷後，應立即停止利用其個人資料宣傳、推廣或行銷，並周知所屬人員。

# 非公務機關蒐集、處理或利用特種個資的合法手段

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

# 匿名化與去識別化

- 法務部法律字第10303513040號
  - 依 103 年 10 月 29 日行政院專案會議「虛擬世界發展法規調適工作專案報告」意見交流內容辦理。
  - 按個人資料保護法（下稱個資法）立法目的之一為個人人格權之隱私權保護，唯有生存之自然人方有隱私權受侵害之恐懼情緒及個人對其個人資料之自主決定權（個資法施行細則第 2 條修正理由參照），故個資法所稱個人，僅指現生存之自然人而言（個資法施行細則第 2條），至若已死亡之人或法人之資料（例如公司之營運狀況、財產等）則不屬個資法之保護範圍。
  - 復按個資法第 2 條第 1 款規定，所謂個人資料係指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、...及其他得以直接或間接方式識別該個人之資料。是以，如將公務機關保有之個人資料，運用各種技術予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者，即非屬個人資料，自非個資法之適用範圍。此後，公務機關主動公開或被動受理人民請求提供是類個人資料去識別化後之政府資訊，除考量有無其他特別法限制外，分別依檔案法第 18 條或政府資訊公開法第 18 條等相關規定決定是否公開或提供即可，無須再擔心是否符合個資法所規範之「特定目的內、外利用」的問題。

# 匿名化與去識別化 (續)

- 法務部法律字第10303513040號
  - 又個資法並非規定可直接或間接識別之個人資料，一律均須保密或禁止利用，公務機關及非公務機關對個人資料之利用，原則上雖應於蒐集之特定目的必要範圍內為之（個資法第 16 條及第 20 條第 1 項本文規定），惟有關個人資料基於具體個案情形，得為特定目的外利用之範圍相當廣泛（個資法第 16 條及第 20 條第 1 項但書各款規定，例如：法律明文規定、為增進公共利益...等），若符合上開但書各款所定事由之一，仍得就個人資料為特定目的外之利用，包含適度提供個人資料給其他機關，俾協助其執行法定職務；在個案適用及認定上，不宜過度偏廢、因噎廢食，遽而停止一切個人資料之利用行為，否則將不符合個資法第 1 條所定「促進個人資料之合理利用」之立法目的，影響民眾權益甚鉅。
- 英國Opinoion 05/2014 on Anonymisation Techniquess 意見書
  - 去識別化(de- identification)：已移除任何直接識別資料與資料主體的資訊，代以聯結因子(linkage key)。
  - 匿名化(anonymisation)：以銷毀資料之個人要素，資料與資料提供者不再具備連結關係。

# 匿名化與去識別化 (續)

- 英國2016年 Anonymisation Decision- Making Framework 匿名化決策框架

# 匿名化與去識別化 (續)

- ISO / CNS 29100 & ISO / CNS 29191
  - 匿名化資料：對任何人而言，均無法採取任何合理可能之方法識別特定個人，亦即資料經加工後，毫無保留連結之可能性；至於判斷資料是否達到已經逆名化之程度，仍須評估各種情況而是個案判斷。
  - 擬匿名化資料：以編碼、別名等方式取代識別符，使研究或統計人員得以針對個體資訊進行分析而無須識別個體身份。
  - 擬匿名化資料- 不可逆：此態樣欲使重新識別不具可能性，以非專屬代碼、單向加密或其他技術處理後，使任何人均無法透過資料比對或其他方式再直接或間接辨識個人。
  - 擬匿名化資料- 可逆：以專屬代碼、雙向加密或其他技術處理後，處理後之編碼資料雖無從識別當事人，但原資料保有者仍得透過代碼與原始識別資料對照表或解密工具，還原資料為識別資料

# 直接蒐集個資告知責任

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：
  一. 公務機關或非公務機關名稱。
  二. 蒐集之目的。
  三. 個人資料之類別。
  四. 個人資料利用之期間、地區、對象及方式。
  五. 當事人依第三條規定得行使之權利及方式。
  六. 當事人得自由選擇提供個人資料時，不提供將對其權益之影響。
- 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。

# 間接蒐集個資告知責任

第九條

- 公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。
- 有下列情形之一者，得免為前項之告知：
  一. 有前條第二項所列各款情形之一。
  二. 當事人自行公開或其他已合法公開之個人資料。
  三. 不能向當事人或其法定代理人為告知。
  四. 基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。
  五. 大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。
- 第一項之告知，得於首次對當事人為利用時併同為之。

# 個資告知執行方式

個資法施行細則

第十六條

- 依本法第八條、第九條及第五十四條所定告知之方式，得以言詞、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為之。

## 當事人同意要求

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。

## 個資當事人權利行使

第三條

- 當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：
  一. 查詢或請求閱覽。
  二. 請求製給複製本。
  三. 請求補充或更正。
  四. 請求停止蒐集、處理或利用。
  五. 請求刪除。

第十條

- 公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：
  一. 妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。
  二. 妨害公務機關執行法定職務。
  三. 妨害該蒐集機關或第三人之重大利益。

# 個資當事人權利行使

第十三條

- 公務機關或非公務機關受理當事人依第十條規定之請求，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。
- 公務機關或非公務機關受理當事人依第十一條規定之請求，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。

第十四條

- 查詢或請求閱覽個人資料或製給複製本者，公務機關或非公務機關得酌收要成本費用。

# 個資當事人權利行使與資料控制者管理

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。

# 非公務機關管理責任

個資法施行細則

第二十條

- 本法第十一條第三項所稱特定目的消失，指下列各款情形之一：
  一. 公務機關經裁撤或改組而無承受業務機關。
  二. 非公務機關歇業、解散而無承受機關，或所營事業營業項目變更而與原蒐集目的不符。
  三. 特定目的已達成而無繼續處理或利用之必要。
  四. 其他事由足認該特定目的已無法達成或不存在。

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實施辦法

第十四條

- 學校、機構業務終止後，其保有之個人資料之處理方式及留存紀錄如下：
  一. 銷毀：銷毀之方法、時間、地點及證明銷毀之方式。
  二. 移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。
  三. 刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。

# 非公務機關管理責任

個資法施行細則

第十九條

- 當事人依本法第十一條第一項規定向公務機關或非公務機關請求更正或補充其個人資料時，應為適當之釋明。

第二十一條

- 有下列各款情形之一者，屬於本法第十一條第三項但書所定因執行職務或業務所必須：
  一. 有法令規定或契約約定之保存期限。
  二. 有理由足認刪除將侵害當事人值得保護之利益。
  三. 其他不能刪除之正當事由。

第十四條

- 本法第六條第一項但書第六款、第十一條第二項及第三項但書所定當事人書面同意之方式，依電子簽章法之規定，得以電子文件為之。

# 非公務機關管理責任

第四條

- 受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。

個資法施行細則

第七條

- 受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之。

# 非公務機關管理責任

個資法施行細則第八條

- 委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。
- 前項監督至少應包含下列事項：

| | |
|---|---|
| 一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 | 四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。 |
| 二、受託者就第十二條第二項採取之措施。 | 五、委託機關如對受託者有保留指示者，其保留指示之事項。 |
| 三、有複委託者，其約定之受託者。 | 六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。 |

- 第一項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。
- 受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。

# 非公務機關管理責任

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實施辦法

第九條

- 學校、機構委託他人蒐集、處理或利用個人資料之全部或一部時，應依本法施行細則第八條規定對受託者為適當之監督，並明確約定相關監督事項及方式。

# 非公務機關管理責任

第二十七條

- 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。
- 中央目的事業主管機關得指定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。
- 前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。

# 非公務機關管理責任

個資法施行細則第十二條

- 本法第六條第一項但書第二款及第五款所稱適當安全維護措施、第十八條所稱安全維護事項、第十九條第一項第二款及第二十七條第一項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。
- 前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：

| | |
|---|---|
| 一、配置管理之人員及相當資源。 | 七、認知宣導及教育訓練。 |
| 二、界定個人資料之範圍。 | 八、設備安全管理。 |
| 三、個人資料之風險評估及管理機制。 | 九、資料安全稽核機制。 |
| 四、事故之預防、通報及應變機制。 | 十、使用紀錄、軌跡資料及證據保存。 |
| 五、個人資料蒐集、處理及利用之內部管理程序。 | 十一、個人資料安全維護之整體持續改善。 |
| 六、資料安全管理及人員管理。 | |

# 非公務機關管理責任

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實施辦法

第五條

- 學校、機構得指定或設管理單位，或指定專人，負責個人資料檔案安全維護；其任務如下：
  一. 訂定及執行安全維護計畫，包括業務終止後個人資料處理方法。
  二. 定期就個人資料檔案安全維護管理情形，向管理人提出書面報告。
  三. 依據稽核人員就計畫執行之評核，於進行檢討改進後，向管理人及稽核人員提出書面報告。

第七條

- 學校、機構應依已界定個人資料之範圍與蒐集、處理及利用流程，分析評估可能產生之風險，訂定適當之管控措施。

# 非公務機關管理責任

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實施辦法

第十二條

- 學校、機構對所保有之個人資料檔案，應設置必要之安全設備及採取必要之防護措施。
- 前項安全設備或防護措施應包括下列事項：
  一. 紙本資料檔案之安全保護設施及管理程序。
  二. 電子資料檔案存放之電腦或自動化機器相關設備，配置安全防護系統或加密機制。
  三. 訂定紙本資料之銷毀程序；電腦、自動化機器或其他儲存媒介物需報廢汰換或轉作其他用途時，應採取適當防範措施，避免洩漏個人資料。



# 非公務機關管理責任

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實施辦法

第十三條

- 學校、機構為確實保護個人資料之安全，應對其所屬人員採取下列措施：
  一. 依據業務作業需要，建立管理機制，設定所屬人員不同之權限，以控管其接觸個人資料之情形，並定期確認權限內容之適當性及必要性。
  二. 檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。
  三. 要求所屬人員妥善保管個人資料之儲存媒介物，並約定保管及保密義務。
  四. 所屬人員離職時取消其識別碼，並應要求將執行業務所持有之個人資料（包括紙本及儲存媒介物）辦理交接，不得攜離使用，並應簽訂保密切結書。

第十五條

- 學校、機構對於個人資料蒐集、處理及利用應符合本法第十九條及第二十條規定，並應定期或不定期對其所屬人員施以教育訓練或認知宣導，使其明瞭個人資料保護相關法令規定、責任範圍、作業程序及應遵守之相關措施。

## 非公務機關管理責任

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實施辦法

第十六條

- 學校、機構應訂定個人資料檔案安全稽核機制，定期或不定期檢查安全維護計畫所定相關事項是否落實執行。

第十七條

- 學校、機構執行安全維護計畫各項程序及措施，應保存下列紀錄：

| | |
|---|---|
| 一、個人資料之交付及傳輸。 | 七、所屬人員違反權限之行為。 |
| 二、個人資料之維護、修正、刪除、銷毀及轉移。 | 八、因應事故發生所採取之措施。 |
| 三、提供當事人行使之權利。 | 九、定期檢查處理個人資料之資訊系統。 |
| 四、存取個人資料系統之紀錄。 | 十、教育訓練。 |
| 五、備份及還原之測試。 | 十一、安全維護計畫稽核及改善措施之執行。 |
| 六、所屬人員權限之異動。 | 十二、業務終止後處理紀錄。 |

## 非公務機關管理責任

第十二條

- 公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

個資法施行細則

第二十二條

- 本法第十二條所稱適當方式通知，指即時以言詞、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為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。
- 依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。

## 非公務機關管理責任

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實施辦法

第八條

- 學校、機構應訂定應變機制，在發生個人資料被竊取、洩露、竄改或其他侵害事故時，迅速處理以保護當事人之權益。
- 前項應變機制，應包括下列事項：
  一. 採取適當之措施，控制事故對當事人造成之損害。
  二. 查明事故發生原因及損害狀況，並以適當方式通知當事人。
  三. 研議改進措施，避免事故再度發生。

## 從當事人角度看組織應有的個人資料保護

### - 以BS 10012: 2017標準

bsi.

# Step 0：確保個人資料被安全的蒐集、處理與利用

Clause 8.2.11 安全議題

- 目標：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。
  - 8.2.11.1 安全措施
  - 8.2.11.2 安全控制
  - 8.2.11.3 儲存與處理
  - 8.2.11.4 傳輸
  - 8.2.11.5 存取控制
  - 8.2.11.8 個人資料移轉到境外其他地區
  - 8.2.11.9 依第三方請求揭露
  - 8.2.11.10 委外處理個人資料

# Step 0：確保個人資料被安全的蒐集、處理與利用

Clause 8.2.2.1 個人資料盤點

- 應維持一份個人資料盤點清冊，盤點清冊亦應載明所使用各類個人資料的目的。
- 組織應記錄個人資料流向在組織的哪些過程。

Clause 8.2.3.1 風險評鑑與處置

- 組織應實行評估處理個人資料對自然人的風險程度的過程，透過隱私衝擊分析來執行。此等評估應包括透過其他組織處理的個人資料。組織應實施風險處置計畫來管理風險評鑑所辨識的任何風險，以降低不符合個人資訊管理系統政策的可能性。
- 風險評鑑過程應包括適當程序，讓可能對自然人造成損害及/或痛苦的任何個人資料處理能夠向上呈報，由負責個人資訊管理及承擔相關責任的人員來檢討。

# Step 0：確保個人資料被安全的蒐集、處理與利用

Clause 8.2.4 訓練和意識

- 組織應確保人員在持續監督下符合個人資料保護法要求與優良實務，含下列事項：
  - 組織應確保這些人員能夠證明他們確實了解個人資料保護法及優良實務，以及個人資料保護法及優良實務應如何在組織內實施；
  - 確保此等人員在適當時與外部機關聯絡，以持續獲知與個人資訊管理有關的議題。
- 組織應能證明所有人員了解自己的責任，並考量相關的安全要求，以確保個人資料是在符合可適用的程序下受到保護和處理。
- 所有人員均應接受訓練，讓他們有能力根據可適用的程序處理個人資料。訓練應適合每位人員在組織內執行的角色。特別要強調，所有人員需遵守適用的資訊安全程序要求。

# Step 1：釐清法源依據

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。

# Step 2：確認特定目的

Clause 8.2.7.1 處理的基礎

- 個人資訊管理系統應確保個人資料僅為一個或一個以上具體指明的目的而取得，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。
- 個人資訊管理系統應確保個人資料不會以違反或可能違反任何法律義務之方式被處理，包括法律規定、普通法或合約條款的義務。
- 個人資訊管理系統應確保為具體指明之目的所蒐集的個人資料不會用於任何其他不相容的目的，但以下情況不在此限：
  a) 適用免除法律義務的情況；
  b) 如組織欲為新目的處理個人資料，該個人資料所屬之自然人已同意組織為該新目的處理其個人資料。
- 個人資訊管理系統應確保高風險個人資料用在相容的新目的時，組織在處理前已獲得自然人之明確同意，但免除此義務時則不在此限。

# Step 3：需要被蒐集的個人資料種類

Clause 8.2.8.2 相關且不過度

- 個人資訊管理系統應確保：
- 組織在為達到合法目的所需要的範圍內，處理最少的個人資料；
- 不處理不相關或對具體目的而言是多餘的資料，除非自然人選擇提供此等資料，且僅在自然人同意下處理此等資訊；
- 檢討個人資訊處理的相關新系統及過程，以確保處理的資料是相關且不過度的。
- 如個人資料對組織的目的而言是不相關或不需要的，個人資訊管理系統應確保此等個人資料不會被處理。
- 備註：組織需考量在處理前要使用匿名或去除其他足茲識別個人資料的方式來進一步保護資料，並記錄其考量的結果。

# Step 4：透過告知取得必要資訊

## Clause 8.2.6.1 個人資料的蒐集與處理

- 個人資訊管理系統應確保以合法為基礎來處理：
  a) 組織公平與合法地處理個人資料；
  b) 組織僅在正當的範圍內處理個人資料；
  c) 僅在基於組織之目的所需要，處理高風險個人資料；
  d) 組織以適當的形式提供隱私權資訊予自然人，當中應明確溝通下列事項：
    1) 組織的身份及其代表的身份；
    2) 個人資料處理的目的；
    3) 組織的合法利益或處理的合法基礎；
    4) 蒐集的個人資料類型(僅當資訊來源為自然人以外時)；
    5) 個人資料來源及是否來自可公開存取的來源(僅當資訊來源為自然人以外時)；
    6) 個人資料露給第三方之相關資訊；
    7) 個人資料轉移到境外時，對現行防護措施的說明，以及如何取得這些防護措施的副本；
    8) 當組織在境外時，組織在國內的聯絡窗口；

# Step 4：透過告知取得必要資訊

## Clause 8.2.6.1 個人資料的蒐集與處理

- 個人資訊管理系統應確保以合法為基礎來處理：
  d) 組織以適當的形式提供隱私權資訊予自然人，當中應明確溝通下列事項：
    9) 在網站上蒐集個人資料所使用的任何技術之細節，例如：cookies；
    10) 讓處理過程公平與透明的任何其他資訊，包含：
      ① 保存期限或是設定保存期限之準則；
      ② 關於自然人近用權、更正權、刪除權、限制個人資料使用權，以及資料可攜權的資訊；
      ③ 向主管機關提出申訴的權利；
      ④ 當處理是基於同意下，可以撤銷同意的權利；
      ⑤ 當資訊的提供是依據法規或是合約要求時，提醒自然人為何必須提供與無法提供資訊之後果；
      ⑥ 有關資訊可能用於任何自動化決策和 / 或剖析的資訊，包括所涉及的邏輯和對自然人的後果。

# Step 5：表達拒絕接受行銷後的尊重

Clause 8.2.6.1 個人資料的蒐集與處理

- 如組織為了行銷目的或未來可能用於行銷目的而蒐集個人資料，個人資訊管理系統應確保向自然人清楚解釋其可拒絕此等行銷的方法。
- 如基於行銷目的使用自動化方式來剖析，個人資訊管理系統應確保向自然人清楚解釋其可拒絕的權利，以及拒絕此等處理的方法。
- 個人資訊管理系統應確保，如根據個人的同意來處理資訊，需留存同意之紀錄。此外，如果撤回同意，則處理基於同意被終止，並保留撤回同意的紀錄。
- 在其他部門要求或法規要求明確同意行銷的情況下，個人資訊管理系統應確保蒐集該同意的細節。
- 如組織為特定目的蒐集高風險個人資料，個人資訊管理系統應確保隱私權資訊明確陳述高風險個人資料被使用或可能被使用之目的。
- 個人資訊管理系統應確保新的蒐集方法會經由適當資格或經驗的人員檢視並簽核，以確保此等方法可被證明是符合個人資料保護要求及優良實務。

# Step 6：行使法律保障權利時的回應

Clause 8.2.12.1 回應其權利

- 個人資訊管理系統應包括確保自然人與其個人資料有關的權利受到尊重的程序，並且在收到自然人的請求後於時限內，無不當延遲地滿足執行該權利的請求。
- 個人資訊管理系統應確保遵守要求，如有需延長該時限，自然人應被告知，並依自然人請求以電子或紙本格式提供影本。個人資訊管理系統應確保符合遵守自然人請求延長該期限，任何延期不超過展延期限。
- 備註：自然人權利包括個人資料近用權、反對處理權、補正不正確資料、刪除和 / 或限制使用個人資料、個人資料可攜權，以及當處理涉及剖析或重大影響自然人時，禁止自動處理的權利。
- 個人資訊管理系統應確保程序包括考慮是否適用任何排除條款。

# Step 7：確保處理個人資料的品質

Clause 8.2.9.1 正確且最新

- 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：
  a) 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；
  b) 在需要時將任何更正的個人資料分享給第三方。

# Step 8：無需再使用後能適當處置個人資料

Clause 8.2.10.1 保留時程

- 個人資訊管理系統應參考個人資料保留期限的保留時間表。保留時間表應包含：
  a) 包括法律要求的最低保留時間及組織規定的保留時間；
  b) 清楚記錄保留時間的正當理由和依據
- 在保留時間到期時，個人資訊管理系統應確保組織不再需要所有個人資料複本都被處置，此等處置過程的管理應符合以下條件：
  1) 使用獲得核准的過程；
  2) 具有適合於個人資料敏感度的安全保障程度；
  3) 與組織的資訊安全風險評估一致。
- 如果要將個人資料轉為給長時間保存，例如：公共利益、科學或歷史研究目的或統計目的，則應採取適當的技術上和組織上措施，維護自然人的權利和自由。
- 個人資訊管理系統應確保實行保留時間表，並傳達給相關的所有人員。

# Step 9：出事時能收到警示通知

## 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：
  - a) 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；
  - b) 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。此類通知應包括下列事項：
    - 1) 事件所涉及的個人資料；
    - 2) 個人資料類別的詳情和涉及的大致總數；
    - 3) 組織資料保護官或其他聯絡據點的聯繫方式；
    - 4) 此一安全事件可能的影響；
    - 5) 描述為解決此一安全事件而採取或提出的措施，並減輕任何可能的不利影響；

# Step 9：出事時能收到警示通知

## 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：
  - c) 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下列事項：
    - 1) 安全事件；
    - 2) 安全事件的性質；
    - 3) 為減輕任何不利風險的行動的任何建議；
  - d) 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；
  - e) 決定是否將安全事件通知主管機關；
  - f) 記錄任何核發的通知。


bsi.

...making excellence a habit.™