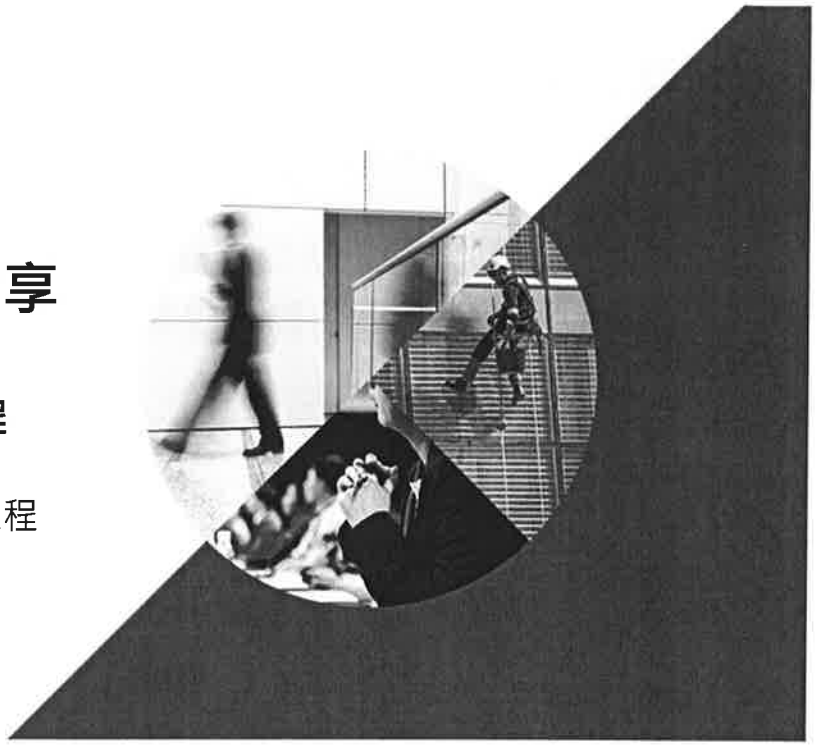
bsi.

個人資料保護
實務經驗分享



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

課程大綱

- 前言
- 重溫2015年12月新修個人資料保護法
- 組織在治理上應有的個人資料保護作為
- Q&A

前言

bsi.

1 英國監管機構確認，DeepMind 非法使用病人資料

科技新報 2017.07.05

- 據英國資料監管機構的報告稱，Google 旗下子公司 DeepMind 與多家英國醫院之間的資料共享協議不符合資料保護法規，英國資訊管理機構在進行長達一年的調查後做出裁定，DeepMind 從英國皇家自由信託基金獲得了 160 萬病人的資料，分別來自 3 所倫敦的醫院。
- 據悉 DeepMind 與英國皇家自由信託基金的資料共享協議在 2015 年年初達成，這一協議已經被新的協議取代。2015 年 DeepMind 正在研發 Streams 應用程式，該程式是從病人的醫療紀錄中獲取資料，對於病人可能出現的健康問題及時向醫生發送警報，Streams 主要用於危及生命的疾病，比如急性腎損傷、尿毒症、肝功能等器官功能衰竭疾病。 DeepMind 已經將 Streams 推廣到多家倫敦醫院，新的資料共享協議比 2015 年的版本範圍更寬泛。
- 2016 年，DeepMind 曾與英國國家醫療服務體系 NHS 旗下基金會 Royal Free London 簽訂了為期 5 年的合約，NHS 旗下的 3 家倫敦醫院將向 DeepMind 分享 172 萬患者的醫療數據。

1 英國監管機構確認，DeepMind 非法使用病人資料

- 資訊管理機構在 DeepMind 與英國皇家自由信託基金的協議中發現了一些漏洞，病人無法完全了解他們的個人資料將被如何使用，負責此次調查的官員 Elizabeth Denham 在聲明中稱，創新能夠給病人帶來幫助，但不一定需要以犧牲個人的隱私權為代價。
- 在資料共享協議中，沒有任何一個條款提及 DeepMind 使用病人資料之前需要徵得病人的同意，共享的資訊包括病人是否存在藥物過量、墮胎和是否帶有愛滋病病毒等資訊。DeepMind 和英國皇家自由信託基金認為病人默認同意分享這些資訊，所有的資訊都是透過 Streams 應用程式來幫助診斷。
- 監管機構認為 DeepMind 和英國皇家自由信託基金沒有充分告知病人，病人無法合理預知他們的資訊會被如何使用，資料共享的過程需要更透明。
- 在雙方的協議中特別提及，任何病人的資料都不會與 DeepMind 的母公司 Google 分享，後者在 2014年收購了 DeepMind，Streams 也沒有應用任何人工智慧技術來分析這些資料，儘管 DeepMind 與英國兩家醫院達成了共同開發用於改善癌症治療和眼部疾病的人工智慧演算法。

1 英國監管機構確認，DeepMind 非法使用病人資料

- DeepMind 發表聲明稱，在原有的協議中確實確定一些漏洞，該公司需要向病人和大眾更充分地解釋這一協議，資料共享協議存在的問題將會很快解決。
- 監管機構認為許多像皇家自由信託基金這樣的機構急於創新，在啟動一些專案時不應該忘記遵守法規，該信託基金已經被要求簽署一項新的協議，承諾審計 2015 年的交易。

2 擔心個資外洩 第三類謄本更安全

自由時報 2017.07.07

- 許多民眾都因舊制謄本揭露資訊過分詳細、開放任何人申請，土地開發業者或仲介業者可能據此登門叨擾，台北市地政局表示，第二類謄本的資訊蒐集、處理及利用應依照個資保護法規定，以避免觸法，並提醒民眾有需要時，使用新制的第三類謄本更能保護個人隱私。
- 地政局指出，新制三類謄本實施前已合法申請下載二類謄本者，由於包含登記名義人的完整姓名、統一編號及住址資料，謄本資訊的蒐集、處理及利用，應依照個人資料保護法規定，以避免觸法。內政部已修正「土地登記規則」第24條之1條文，自2015年2月2日起，原規定任何人皆能申請的第二類土地登記謄本，改以去識別化方式，僅公開所有權人的姓氏、部分國民身分證統一編號，但仍保留完整住址資料，以促進土地利用及整合開發需要，民眾假如有疑慮，也可請求隱匿部分地址資料，並新增利害關係人才能申請的第三類土地登記謄本，增加謄本分級，保護個資安全。

2 擔心個資外洩 第三類謄本更安全

- 新制三類謄本依照申請人資格不同，將謄本分為三類：第一類謄本，顯示登記名義人全部資料，限登記名義人或其代理人才可申請；第二類謄本，隱匿登記名義人的出生日期、部分姓名、部分統一編號、債務人及債務額比例、設定義務人及其他依法令規定需隱匿資料，任何人都能申請；第三類謄本，隱匿登記名義人的統一編號、出生日期，限利害關係人才可申請。

謄本種類	申請資格	謄本內容揭露 ✓全部顯示 △部分顯示 ✗不顯示				
		姓名	出生日期	統一編號	住址	債務人及債務額比例及設定義務人
第1類	登記名義人或其他依法令得申請者	✓	✓	✓	✓	✓
第2類	任何人	△ 陳＊＊	✗	△ A123＊＊＊＊9	✓	✗
第3類	登記名義人利害關係人	✓	✗	✗	✓	✓

3 社群資料永生 引發爭議

聯合財經網 2017.06.24

- 我們上傳到社群網站如臉書（Facebook）、推特（Twitter）和領英（LinkedIn）的資料內含大量個人訊息，包括平日生活、常去的地方、嗜好、經常往來的人士是誰等等。
- 基於隱私顧慮或情感因素，想保護這些資料是人之常情，甚至會希望了解，當生命消逝後，各大社群網站如何處理這些帳號資料？將來這些資料可能落入何人之手？

臉書

- 富比世雜誌報導，臉書2015年推出遺贈功能，在臉書被通知用戶逝世後，受用戶請託的人便可選擇關閉帳號或轉為紀念模式。一旦轉成紀念模式，這個帳號會被「凍結」，只有該用戶之前的臉書好友才能看見，發文也不能增加或刪除。
- 去年臉書增加了新功能，在臉書確認用戶離世後，受託人可在有限範圍內使用已逝用戶的帳號，在首頁選定值得紀念的訊息或張貼葬禮訊息，也可下載某些個人資料，但不能碰私密訊息。臉書沒有公開表明用戶死後訊息資料會留存多久、可不可能永久刪除。

3 社群資料永生 引發爭議

推特

- 乍看下，推特的處理方式比較直截了當。用戶若逝世，死者的近親或是遺囑執行人可要求移除帳號，但沒有如同臉書那樣的紀念模式。然後帳號會被停用，意味被列入帳號準備刪除的名單。但推特並不保證該帳號會從系統永久移除，有可能會留下備份檔。

LinkedIn

- LinkedIn因為是商業交流網站，處理方式也不同。任何人都能以某用戶死亡的理由，申請刪除其個人檔案（profile）。身為專業商業社群網站，LinkedIn沒有提供紀念模式或保存檔案，根據LinkedIn條款，個人檔案就是直接「移除」。
- 特別的是LinkedIn用的字眼，例如移除（remove）、限制（restrict）、取消授權（deauthorize）和關閉（deactivate），都沒有明說資料會不會被刪除。LinkedIn表示當帳號遭移除時，個人檔案也會被刪除，但資料只是不再提供存取。所以可以推斷，已逝用戶的資料仍然存在，在LinkedIn做一些與仍在世者有關的決定時被拿來當作參考。

3 社群資料永生 引發爭議

- 另一個顯著的差異是，LinkedIn沒有一套機制可讓用戶指定人選，授權他使用自己的帳號，或下載個人資料。或許是因為LinkedIn認為用戶在該網站發布的訊息不像在臉書分享的內容那般具情感價值。
- 大型社群網站對保護已逝者隱私的重視，可能更甚於把資料提供給他們的親人。根據網站The Digital Beyond的調查，有80%的人認為已逝者的隱私權凌駕於他人存取已逝者帳號的權利。
- 雖然大型社群網站某種程度上讓用戶能決定自己死後帳號如何處置，但用戶恐怕沒有完全的控制權。目前我們並不能夠選擇將自己的檔案從臉書、推特或LinkedIn的系統完全抹去。

4 幽靈投票？ 美各州拒交選民資料

聯合財經網 2017.07.02

- 美國總統川普曾指有非公民或使用他人身分的人在去年總統大選中投票，因此白宮專責選舉舞弊的委員會要求各州提交共2億選民的資料，但遭各州一面倒地反對，不僅是民主黨執政的州，連共和黨掌政的州也認為白宮反應過度，已有20多個州拒絕呈交。
- 川普本人對此頗感不滿，他1日在推特發文說：「許多州都拒絕提供資訊給非常卓越的選民舞弊委員會。那些州在隱瞞什麼？」
- 川普去年雖因獲得多數選舉人票而入主白宮，但普選票數卻輸給民主黨對手希拉蕊．柯林頓，川普認為是數以百萬計的非法選民投票支持柯林頓，因此成立這個總統顧問委員會。委員會副主席柯巴克曾致函要求選舉官員交出有關數據，目的顯然要在全國找非法選民投了票的證據。
- 除了選民基本資料，例如姓名及所屬政黨之外，委員會還要求提交個人資料，包括出生日期、犯罪紀錄、過去十年的投票歷史、社安號的最後幾個數字等。

4 幽靈投票？ 美各州拒交選民資料

- 本身是堪薩斯州務卿的柯巴克表示，他希望這些資料能夠比對選民資料，例如外國居民及無證移民的聯邦紀錄等。儘管目前找到的證據不多，但他仍然確信這些非法選民不在少數。
- 不過各州愈來愈多選舉官員，婉轉或直接的表示，他們不會或不能提供這些資料；紐約時報報導，諷刺的是，就連柯巴克及委員會第二號人物、印第安納州務卿康妮．勞森都透露，隱私法禁止收集個人的選舉資料。
- 報導說，至少22個州的選舉官員已部分或完全拒絕委員會的要求。加州、麻州、維吉尼亞、紐約及肯塔基等州都拒絕要求。

5 美國史上最嚴重！ 近2億選民個資慘遭外洩

自由時報 2017.06.20

- 近2億美國公民的個資傳出外洩！美國資安研究人員指出，川普共和黨陣營的資料承包公司讓約1億9800萬美國人的個資曝光，幾乎涵蓋所有合格登記的美國選民。
- 綜合外媒報導，資安公司「Upguard」研究人員表示，他們發現1個未對雲端資料庫做任何防護措施的數據庫，內容涵蓋由「深根分析公司」（Deep Root Analytics）替共和黨全國委員會（Republican National Committee）承包的選民個人資料，共有多達100億頁文字檔，這是目前已知最大宗美國選民個資外洩案。
- 報導指出，洩漏出的個資非常詳細，包括「姓名、生日、住家地址、電話號碼和選民登記細節」，名單還涵蓋選民到投票意向等，該資料庫被視為川普陣營在選戰期間的寶庫，整份名單佔了全美62%的人口數，約1億9800萬人受害。
- 深根分析公司表示，此次非被駭客入侵，公司願意承擔所有責任，現正與外部專家合作調查。對此「Upguard」則認為，如此龐大的網上國家數據庫，連基本保護措施都沒做好，另外私人企業竟可得到大量的個資，也令人感到不安。

5 選舉處失電腦 載全港選民選委資料

明報新聞網 2017.03.28

- 特首選舉剛落幕，不過選舉事務處昨日發現，存放於特首選舉後備場地亞洲博覽館的兩部手提電腦懷疑失竊，分別載有 1194 名選委以及全港選民個人資料。選管會昨已向警方報案，並通知個人資料私隱專員公署。有泛民選委昨斥事件「匪夷所思、國際笑話」，要求選管會交代。大批警員昨晚赴亞博館地氈式搜查。警方表示案件暫列盜竊，由新界南總區重案組跟進。
- 政制及內地事務局昨表示，晚上 8 時半收到選管會通知，已責成選舉事務處全面配合警方調查。

上鎖房間內失竊 警大搜亞博

- 特首選舉周日於灣仔會展中心舉行，選舉事務處昨晚 10 時多發新聞稿，稱處方在機場亞洲國際博覽館設後備場地，事後發現館內一個上鎖房間的兩部手提電腦懷疑失竊，已報警。兩部電腦中，一部載有選舉委員會委員的全名，另一部則有地方選區選民姓名、地址及身分證號碼，資料已根據保安要求加密處理。

5 選舉處失電腦 載全港選民選委資料

載選民姓名地址身分證

- 選舉事務處發言人表示，「暫時沒有資料顯示相關資料有外泄情況」，強調選舉事務處一向十分謹慎處理選民登記資料，非常重視保安，職員均嚴格遵從政府和相關機構就處理重要個人資料保安的法例、守則和加密要求。
- 獲口頭通知的私隱專員公署昨表示，留意到當中可能涉及個人資料數量頗大，會就事件展開循規審查，並建議處方應盡快澄清事件具體內容，適當通知涉事者。

議員斥「國際笑話」 質疑資訊安全

- 根據政府數字，2016 年本港共有約 378 萬名登記選民。民主黨林卓廷昨直斥，全港選民個人資料遺失屬「國際笑話，匪夷所思」，譴責選舉事務處漠視市民私隱。他又表示，令人百思不得其解的是，特首選舉只有 1194 人有票，「選舉事務處帶全港市民資料去會場做什麼呢？」民主黨將就事件要求召開政制事務委會特別會議，促選舉事務處盡快交代。資訊科技界立法會議員莫乃光亦斥，選舉事務處不小心處理如此大量資料，不能接受，認為選管會資訊安全基本程序極有問題。

6 蒐集個資嚇到網友　花唄緊急滅火

中時電子報 2017.07.07

- 螞蟻金服旗下金融借貸產品「花唄」，最近新版用戶合約在網路上曝光，其中戶籍、社會保險、通話等個人資料的授權條款，引發大陸網友熱烈討論。有網友坦言「被嚇到了」，考慮乾脆棄用花唄。
- 近日，一篇名為《支付寶＜花唄＞新版合同，讓人不寒而慄，都要蒐集「手機通話分鐘數了」》的網路文章，在大陸引起爭議。該文章引用花唄6月30日剛公布的用戶合約，上面清楚寫道，「為了蒐集個人訊息，支付寶要蒐集個人手機號碼的餘額、通話對象、通話分鐘數了。」
- 此外，根據《南方都市報》報導，螞蟻金服還打算蒐集用戶的戶籍訊息、社保參保狀態、銀行帳戶和信用卡資訊。有人擔心，在這樣下去，未來所有個資都會淪為企業大數據所用，「後果是什麼，現在想想都不寒而慄。」

6 蒐集個資嚇到網友　花唄緊急滅火

- 網友反應一面倒的負評，時隔幾天，花唄立刻修改用戶合約，3日已正式生效。花唄4日也在官方微博發文滅火，強調蒐集用戶訊息是為了降低風險，了解借貸人的財務跟信用狀況，並決定放貸額度，是業內的常態作法。實際蒐集的個資範圍會「遠小於此」。
- 不過，對於花唄的說法，一些律師並不買單，認為有違個資法之嫌。大陸個資法都寫在6月1日上路的《網絡安全法》中，要求業者收集和使用個人訊息需要遵守合法、正當、必要性原則。
- 中國電子商務研究中心特約研究員、浙江嫚丁律師事務所聯合創辦人麻策表示，花唄顯然有過度蒐集個資的嫌疑。特別是社保訊息和通話記錄，北京志霖律師事務所副主任趙占領說，「即使銀行貸款也未收集這類信息。」

7 BMW推CarData服務可供第三方業者使用

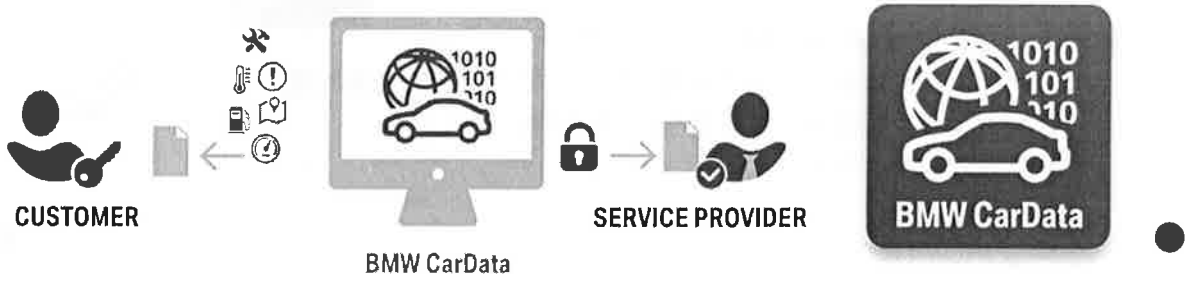
DIGITIMES 2017.06.21

- BMW宣布推出BMW CarData，提供汽車數據供保險業者、個人化資訊娛樂等第三方業者使用。註冊過的ConnectedDrive用戶，也可以免費使用BMW CarData。
- Auto Connected Car News報導，內建SIM卡的BMW車型可以提供BMW CarData，目前大約有850萬台BMW汽車符合相關要求。只要一個按鍵，就可以決定是否開放資料、或者拒絕存取資料，也可以撤回之前同意的內容。客戶可以單方面決定第三方公司是否能得到他們的數據，可以完全掌控一切。
- BMW聲稱是第一家推出相關服務的汽車公司，也遵守EU General Data Protection Regulation。客戶可以透過ConnectedDrive連接埠取得CarData報告。相關檔案有詳細的汽車電子數據，而且有一份檔案詳細解釋這些重要詞彙。
- 停車場、保險公司與車隊管理業者等服務供應商可以註冊使用BMW CarData。如果客戶同意開放其汽車電子數據，這些公司就能使用經過BMW加密的數據。這些資訊可以提供客制化的創新服務，包括資訊娛樂系統和智慧家庭功能等，可以發展各種附加服務。

7 BMW推CarData服務可供第三方業者使用

DIGITIMES 2017.06.21

- BMW CarData先在德國推出，並逐漸推廣到其他市場。BMW Connected服務目前已經與Apple Watch、亞馬遜(Amazon)Echo/Alexa、Android和三星電子(Samsung Electronics)Gear S3相容，主要提供汽車駕駛和行人使用。
- BMW Connected Open Mobility Cloud連結智慧型手機、智慧手錶與汽車，把汽車整合到數位生活裡。它會依據個人來判斷用戶的行動模式，並提供個人化的使用體驗。



重溫2015年12月
新修個人資料保護法

bsi.

為什麼要制訂個人資料保護法？

- Nineteen Eighty Four- 1984：是George Orwell創作的一部政治諷刺小說，書中講述了一個令人感到窒息和恐怖的，以追逐權力為最終目標的假想的未來極權主義社會，通過對這個社會中一個普通人Winston Smith的生活描寫，投射出了現實生活中極權主義的本質。

- 無所不在的「老大哥(Big Brother)」
  - 監控(surveillance)
  - 管制(壓迫)、服從
  - 摧毀隱私
- 實務上，Big Brother Model仍有其侷限
  - 資料蒐集目的並非全是為了壓制、服從，即使是政府的資料蒐集也是如此。
  - 社會救助、全民健保、社會福利(老農津貼)
  - 一般私人蒐集資料的目的

為什麼要制訂個人資料保護法？

- Der Prozess- 審判：是Franz Kafka寫的一部長篇小說。小說的主角Josef K在一個早上被喚醒後，不明原因地被捕，陷入一場難纏的官司之中，卻不知道自己的罪名。Josef K最終在一個黑夜裡被帶走，並秘密處死。

- 描述在審判過程中的一種「權力關係(power relation)」
  - 一切都在狀況外
  - 無力感(無法介入整個程序)
  - 套用到目前公務機關或非公務機關蒐集、處理、利用我們個人資料的現實

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。**

組織應有的個人資料保護

- 以BS 10012: 2017標準

bsi.

Step 0：管理層的認同與資源的投入

Clause 5.1 領導與承諾

- 管理高層應藉由下列事項，展現領導與承諾：
  - 確保以建立個人資訊管理系統政策及個人資訊管理系統目標，並與組織的策略方向一致；
  - 確保個人資訊管理系統的要求事項整合進組織的營運過程；
  - 確保個人資訊管理系統所需要的資源可以取得；
  - 傳達有效的個人資訊管理系統的重要性，及符合個人資訊管理系統要求事項的重要性；
  - 確保個人資訊管理系統達成其預期成果；
  - 指導及支援人員，以促進個人資訊管理系統的有效性；
  - 宣導持續改善；
  - 當適用其他相關管理角色的職責範圍時，予以支持以展現其領導力。

Step 0：管理層的認同與資源的投入

Clause 7.1 資源

- 組織應決定並提供建立、實作、維持及持續改善所需資源。

Clause 7.2 能力

- 組織宜採取下列措施：
  - 決定於組織控制下執行工作， 影響其個人資訊管理系統績效人員之必要能力；
  - 確保此等人員於適當教育、訓練或經驗之基礎上能勝任；
  - 於適當時，採取取得必要能力之行動，並評估所採取行動之有效性；
  - 保存適切之文件化資訊，作為勝任之證據。

Step 1：人員對個人資料保護的認知

Clause 7.3 認知

- 於組織控制下執行工作之人員，應認知下列事項：
  - 個人資訊管理系統政策；
  - 其對個人資訊管理系統有效性之貢獻，包括改善之個人資訊管理系統績效的益處；
  - 未遵循個人資訊管理系統要求事項之可能後果。

Clause 5.4 結合組織文化

- 對人員持續進行教育和意識提升，以培養、促進和維持個人資訊管理的意識；
- 建立評估個人資訊管理系統意識傳遞有效性的流程；
- 將以下事項的重要性傳達給所有人員，包含：目標、政策、持續改善；
- 確保所有人員知道他們對達成組織的個人資訊管理系統目標及不遵守的後果；
- 維持訓練與意識活動及其有效性的文件化資訊。

Step 1：人員對個人資料保護的認知

Clause 8.2.4 訓練與意識

- 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(見條款7.3)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 2：掌握所持有的個人資料- 方法

Clause 6.1.2 資料盤點與資料流向

- 建立與維護個人資料盤點與個人資料流向分析，鑑別以下資訊：
  - 主要業務流程所應用的個人資料；
  - 個人資料的來源；
  - 所處理的個人資料分類，包含鑑別高風險個人資料(見條款 8.2.2.2)；
  - 個人資料被運用的目的，包括次要目的中超過原蒐集之初始目的；
  - 潛在個人資料接收方，包括揭露個人資料的第三方、資料處理者及轉移的供應商；
  - 透過個人資料流向，應顯示組織所扮演的資料控制者、資料處理者或資料協同控制者；
  - 個人資料的關鍵系統與存放處；
  - 透過個人資料流向，顯示傳輸至境外或以不同法律、法規、標準或規範的個人資料；
  - 個人資料保留或處置的認可準則要求。
- 確保重複之資料盤點結果產生一致、有效及適用於比較之結果。

Step 2：掌握所持有的個人資料- 執行

Clause 8.2.2 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。

Step 3：瞭解可能的風險- 方法

Clause 6.1.3 隱私衝擊分析

- 組織對處理之個人資料應訂定隱私衝擊分析程序：
  - 建立和維護隱私風險標準，包含：
    風險可接受水準；
    隱私風險評鑑標準；
    為識別隱私風險，可於資料流向中運用資料保護原則。
  - 確保重複之隱私風險分析產生一致、有效及可比較之結果；
  - 識別資料保護風險，與隱私風險分析過程產生關聯，識別風險包含：
    隱私相關法律、標準與框架；
    對自然人的權利與自由所造成的影響；
    對自然人造成任何生理上、物質與非物質上的損害；
    對組織所造成的衝擊，包含但不限於聲譽、法律規章、財務損失等；
  - 識別高風險個人資料(見條款8.2.2.2)及相關高風險個人資料的處理；
  - 識別風險擁有者；

Step 3：瞭解可能的風險- 方法

Clause 6.1.3 隱私衝擊分析

- 組織對處理之個人資料應訂定隱私衝擊分析程序：
  - 分析隱私風險，在於：
    在隱私風險分析中評估所識別風險發生的嚴重性；
    在隱私風險分析中評估所識別風險發生的可能性；
    決定風險等級。
  - 計算隱私風險，包含：
    以風險準則比較風險分析的結果；
    訂定已分析風險之風險處理優先順序。
- 組織應保存關於隱私風險評鑑過程之文件化資訊。

Step 3：瞭解可能的風險- 執行

Clause 8.2.3 風險評鑑和處置

- 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 4：確認法源依據與特定目的

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 4：確認法源依據與特定目的

Clause 6.1.3.2 特種個人資料

- 當需要處理特種個人資料時，需驗證、定義與文件化法源依據方式處理個人資料，可由下選擇至少其中一項：
  - 自然人對特定目的的明確同意；
  - 基於聘僱時必要的權利與義務；
  - 保護自然人重大利害關係；
  - 非營利機構在適當保護下的合法活動下；
  - 經自然人自行公開；
  - 基於法律主張之建立、行使與辯護之必要；
  - 基於合理的重大公共利益；
  - 基於預防或專業醫學、員工能力評估、醫療診斷、健康預防，或社會照護系統與服務；
  - 基於合理公共衛生或執業時保守保密要求；
  - 由國家法律規範之基因、生物或健康資料之處理。

Step 4：確認法源依據與特定目的

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：
  - 適用免除法律義務的情況；
  - 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。

Step 4：確認法源依據與特定目的

Clause 8.2.7.4 資料分享

- 應確保在組織與其他組織分享個人資料時，雙方對個人資料的責任已依照適當情況正式載明於書面協議或合約中。
- 如其他組織為自己的目的使用個人資料時，應確保：
  - 書面協議或合約中載明使用資訊之目的，以及進一步為其他目的使用個人資料的任何限制或約束；
  - 其他組織提供承諾或證據證明其不會以抵觸個人資料保護法的方式處理資訊的承諾。
- 應盡可能確保第三方分享提供自然人的隱私權資訊，如不可能，組織應確保：
  - 有合法資料分享基礎；
  - 以適當的方式，提供合適的分享通知給自然人；
  - 評估目的拘束原則的遵循性；
  - 需要時，取得自然人對資料分享的同意。

Step 5：蒐集、處理與利用的必要範圍

Clause 8.2.8.2 相關且不過度

- 組織應確保：
  - 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。

Step 5：蒐集、處理與利用的必要範圍

Clause 8.2.11.9 依第三方請求揭露

- 應包含適當程序，確保第三方提供下列事項：
  - 申請特定個人資料副本的權利；
  - 必要時確認其身份。
- 個人資訊管理系統應確保組織檢查並確定對第三方揭露任何資訊具有合法基礎。組織應在需要的範圍內，對第三方揭露最少的個人資料。
- 個人資訊管理系統應維護個人資料揭露的紀錄。此等紀錄應能證明揭露是合法的，且應能讓組織持續追蹤個人資料在何處被揭露。

Step 6：必要時隱私權資訊的告知

Clause 8.2.6.1 個人資料蒐集與處理

- 個人資訊管理系統應確保以合法為基礎來處理：
  - 組織公平與合法地處理個人資料；
  - 組織僅在正當的範圍內處理個人資料；
  - 僅在基於組織之目的所需要，處理高風險個人資料；
  - 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：(以下略)
- 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。
- 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 7：確保個人資料的品質

Clause 8.2.9.1 正確且最新

- 應確保被處理之個人資料維持完整和正確性。
- 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，應記錄不正確處並適當提供正確的個人資料。
- 應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。
- 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。
- 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。

Step 8：適當時移除個人資料

Clause 8.2.10.1 保留時程

- 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：
  - 包括法律要求的最低保留時間及組織規定的保留時間；
  - 清楚記錄保留時間的正當理由和依據。
- 在保留時間到期時，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：
  - 使用獲得核准的過程；
  - 具有適合於個人資料敏感度的安全保障程度；
  - 與組織的資訊安全風險評估一致。
- 如要長時間保存，應採適當技術上和組織上措施，維護自然人的權利和自由。
- 應確保實行保留時間表，並傳達給相關的所有人員。

Step 9：個人資料安全蒐集、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 9：個人資料安全蒐集、處理與利用

Clause 8.2.11.3 儲存與處理

- 個人資訊管理系統應確保個人資料受到安全的儲存和處理，並備妥符合於其機密性和敏感度的預防措施。
- 個人資訊管理系統應確保特別關注於將儲存在可移除式媒體、可攜式裝置(特別是在「個人自備裝置 BYOD」政策下所使用的可攜式裝置)，及第三方儲存系統(例如：雲端儲存空間)。

Clause 8.2.11.4 傳輸

- 個人資訊管理系統應確保，當個人資料在組織內部以電子或手動方式傳輸，或傳輸到其他組織時，其傳輸的安全受到組織所定義的適當方法所保障，進而確保傳輸過程中受到適當保護。

Step 9：個人資料安全蒐集、處理與利用

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。

bsi.

...making excellence a habit.™