iThome Studio

iThomeFB粉絲團 開播

大話資安 LIVE

首播強打 GDPR答客問

達成GDPR遵循性的20個步驟

來賓：臺灣BSI總經理 蒲樹盛

來賓簡介：

蒲樹盛總經理專長為資訊安全及營運持續管理，在國際標準及驗證產業擁有近20年的資歷，為業界倡導風險管理之先驅，擅長分析各式風險對企業的衝擊，並提供因應作為與策略規劃的見解。

蒲樹盛總經理在台灣推行資訊安全治理成效斐然，經常受邀為政府部門及民間企業提供指導及建議，並促進產業發展合作，成功將國際標準拓展及建立於政府、電信、金融等行業，奠定了極具領導地位的專業知名度。

目前亦為中華民國電腦稽核協會(CAA)常務理事及行政院資通安全外部委員，並將持續運用 BSI 一世紀來制定管理標準的經驗，引領國內企業組織建置完善的管理流程，邁向永續經營。

GDPR重點解析與企業因應策略

GDPR 遵循性的 20 個步驟

Peter Pu (蒲樹盛), 總經理 , BSI 英國標準協會
Peter.pu@bsigroup.com

UK Superbrands 2018

By Royal Charter

改革的目標

歐盟資料保護規範的改革，有 5 大基本目標， 摘述如下：

- 強化個人權利 – 從設計端保護隱私要求 (Privacy by Design)
- 制定嶄新、清楚且周密的法規，確保個人資料得以合理自由流通
- 確保相關法規實施的一致性
- 樹立全球資料保護的標竿
- 確保一套可適用於各產業的資料保護黃金機制

bsi.

歐盟一般資料保護規範(共11章99條)
General Data Protection Regulation (GDPR)

- 歐洲議會於2016年4月27日通過歐盟法規2016/679，亦即「一般資料保護規範（General Data Protection Regulation, GDPR）」
- 自2016年5月24日起生效，並取代歐盟1995年的 「資料保護綱領」。
- GDPR規定2年過渡期，自2018年5月25日起全面施行新法。
- GDPR不僅適用於歐盟地區註冊的企業，非屬歐盟企業組織但在歐盟境內營運，蒐集、處理或利用歐盟人民的個人資料者均適用本法。
- GDPR提升個資保護強度，大幅提高了罰款金額上限，最高可處罰鍰 2 千萬歐元或年度全球總營業額 4% 的金額。

bsi.

歐盟一般資料保護規範 (GDPR)

以條理化、系統化與邏輯化的方法達成 GDPR 遵循性的 20 個步驟

一套循序漸進的作法:
BSI 建議組織依序採取以下 1 – 20 的步驟，目的是為了幫助組織整合既有的架構

bsi.

步驟類型

BSI 將這 20 個建議步驟分為如下 4 個類別：

- 治理 (Governance) - 6 個步驟
- 技術 (Technical) - 4 個步驟
- 作業 (Operational) - 6 個步驟
- 溝通 (Communicative) - 4 個步驟

Step 1 - 資料保護長 (Data Protection Officer, DPO)

- 第一個步驟就是指派一位資料保護長 (DPO)。實際上，大部份的組織都需要根據其作業流程、規模及組織屬性，正式決議是否需要設立資料保護長。無論組織是否設立一個正式的職位，維護資料保護與隱私權等的職責都必須被正式地指派(需要指派某一人負責資料保護的工作)。
- 為確保「資料控制者 data controller」或「資料處理者data processor」之有效遵循法規，要求設立資料保護長(DPO)。
- 公務機關/ 核心業務涉及到對歐盟居民的資料處理
- 從資料蒐集、處理或利用的性質、規模及/或目的判斷，需要定期、有系統，大規模的監控資料當事人(如: 敏感性個資、犯罪資料...)
- 此一職位並必須有效依法履行職責，若違反GDPR之規範，DPO將被追究法律責任。

bsi.

Step 1 - 資料保護長（Data Protection Officer, DPO）

- 可以採用如下方法：
  - ✓指派某一個既有的員工擔任資料保護長之職
  - ✓增設新的職位進行招聘
  - ✓委由第三方單位派遣出任資料保護長
- 無論採用哪種方式符合規範要求，組織都有兩種義務，包括：
  - ✓確保資料保護長符合所有必要的訓練及能力要求
  - ✓確保所指派的資料保護長與組織的營運業務沒有任何利益衝突
  - 許多組織由於缺乏資料保護領域的相關技能，使得具備資料保護長工作經驗，以及具有相關證照資格者的薪資水準較高，對組織而言，設立這項職務格外具有挑戰性。同樣地，由外部委任派遣資料保護長所需花費的成本，也將成為組織額外的成本負擔。
  - 針對既有員工加以訓練來補足這些技術缺口，可能會發生受訓中的資料保護長給予的建議尚不夠專業，而導致相付出昂貴代價。此外，在訓練過程中，既有員工也可能無暇繼續兼顧原本的日常工作，組織同樣需要考量這類機會成本對營運所帶來的利益衝突。

Step 2 - 權責義務

- 相關的資料保護權責義務，必須在整個組織內所有與資訊處理相關的活動中，被明確地分派、說明與呈現。
- 達成此目的的最佳方法，是指定各個負責處理資訊之事業單位主管 / 代表來承擔資訊持有者的責任。
- 幸而大部份的組織就算未正式展開行動，也已瞭解各事業單位中涉及個人資料處理的各方職責。此步驟最重要的，就是確保相關的責任與權利，已經納入資訊持有者應承擔的職責內。
- 要達成這項目標，可以透過要求資訊持有者製作資料 / 資訊盤點清冊及資料 / 資訊流圖表 (詳步驟 3 與 4)。

bsi.

Step 3 - 資料 / 資訊盤點清冊

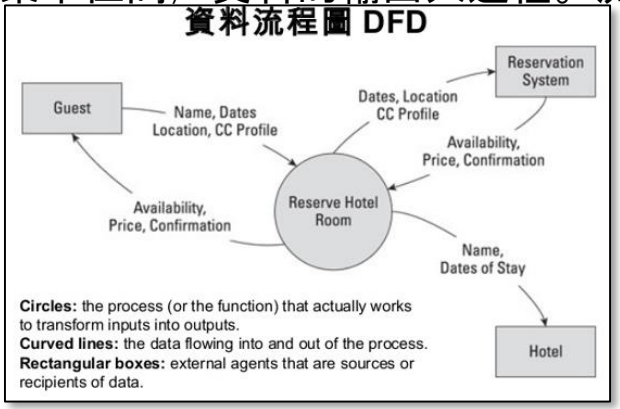
- 在啟動資料保護計畫時，最重要的就是牢記「您無法保護您所不瞭解的資料」，因此，確實認識您所持有的資料之歷程。
- 資料暫存格式與結構須先達成一致的共識，組織所持有或處理的個人資料，都必須依據此格式紀錄於盤點清冊中。
- 資料 (或資訊) 盤點清冊至少須被記錄以下內容：
  - ✓存放個人資料之系統名稱
  - ✓該資料的分類方式
  - ✓處理該資料的目的
  - ✓處理該資料所依循的法源基礎
  - ✓資料的留存時限
  - ✓資料所涉及的特定主題或類別
  - ✓資料持有者 (Data owner)
  - ✓如有第三方單位共享資料，其身份為何

基本資訊					
作業流程名稱/資訊系統模組	單位名稱	特定目的之項目	個人資料類別	個人資料檔案名稱 (若無具體名稱請概述用途)	資料筆數
註冊流程	資訊部	行銷	身分證、職稱、住址	客戶名單_201001	100
註冊流程	資訊部	行銷	身分證、職稱、住址	客戶名單_201002	23
註冊流程	資訊部	行銷	姓名、身分證、職稱、住址	客戶名單_201101	74
註冊流程	資訊部	行銷	姓名、身分證、職稱、住址	客戶名單_201102	77
註冊流程	資訊部	行銷	姓名、身分證、職稱、住址	客戶名單_201103	1500
註冊流程	資訊部	行銷	姓名、身分證、職稱、住址	客戶名單_201104	463
註冊流程	資訊部	行銷	姓名、身分證、職稱、住址	客戶名單_201105	462
註冊流程	資訊部	行銷	姓名、身分證、職稱、住址	客戶名單_201106	105
註冊流程	資訊部	行銷	姓名、身分證、職稱、住址	客戶名單_201107	102
註冊流程	資訊部	行銷	姓名、身分證、職稱、住址	客戶名單_201108	112
註冊流程	資訊部	行銷	姓名、身分證、職稱、住址	客戶名單_201109	340
註冊流程	資訊部	行銷	姓名、身分證、職稱、住址	客戶名單_201110	324
註冊流程	資訊部	行銷	姓名、身分證、職稱、住址	客戶名單_201111	354

- 如步驟 2 中所顯示，這些工作將必須由資料持有者完成，並由資料保護長從嚴審查。

Step 4 - 資料流程圖

- 組織最重要的工作是確保所有利害關係人，都能夠明確、快速且正確的理解其個人資料將被如何處置。無法光靠步驟 3 中所提及的盤點清冊來達成此目的，為了彌補不足的部分，使用流程圖來呈現，是最容易讓人理解的方式。
- 流程圖可呈現出每一項資料處理作業活動或事業單位間，資料的輸出入過程。流程圖必須包含：
  - ✓資料細節
  - ✓資料是如何以及從何處獲得
  - ✓資料儲存於何處
  - ✓資料在組織內哪些單位間傳遞
  - ✓負責處理資料之系統名稱
  - ✓可能傳輸資料的第三方單位細節資訊 (包括所使用的安全措施，例如：加密)
  - ✓資料將如何以及何時銷毀



- 流程圖的繪製將必須由資料持有者進行，並由資料保護長從嚴審查。
- 這類流程圖帶來的實質效益之一，是能夠幫助組織迅速掌握資料的位置，並有助於即時回應資料主體行使權利，例如：近用權，或刪除權等要求時。(請參考步驟 9 及 10)

Step 5 - 資料適足性與適量性

- 現在您已經瞭解組織所握有的資料，可以開始思考該資訊的適足性與所蒐集之資訊的範圍。
- 以更加嚴格謹慎的角度，審查所有盤點清冊/資料流程圖中的資料。組織需要審視所有的資料，並自我詢問：「是否真的需要此資料？」以及「我們如何取得此資料？」以及「資料是否使用得當？」
- 如果資料並非絕對有需要，請刪除並且停止蒐集。
- 維護的資料越少，就長期而言，您在資料保護的遵循性上，所需花費的精力便越少。

bsi.

Step 6 - 資料處理者

- 如果您所蒐集的資料需透過廠商處理，則必須確保適度的安全性以及隱私協議都已提列在正式合約中，經雙方共同簽署並確實執行。
- 最理想的狀況是，這些合約所包含的條款內容，可確保廠商得以安全且保密的方式來處理資料，符合相關隱私規範，並得以讓您進行稽核且隨時抽查，以確保合規性。
- 資料控制者常見的做法是，要求廠商（資料處理者）提出通過驗證的證明，或至少符合某一資訊安全標準，例如：ISO / IEC 27001 資訊安全管理系統、BS 10012 個人資訊管理系統

bsi.

Step 7 - 同意管理

資料蒐集與處理須取得明確有效同意

- 強化同意書的條件，公司將不可再使用充滿法律術語及難以了解的條款與細則。同意書必須是以可理解且容易存取的形式提供，並包括資料處理用途，且能明確與其他事項區分。
- 撤銷同意書必須和提供同意書一樣容易

可理解、易接近

單獨同意

撤銷容易

- 臺灣個資法規定相同
- 消保法施行細則第12條：定型化契約條款因字體、印刷或其他情事，致難以注意其存在或辨識者，該條款不構成契約之內容

Step 7 - 同意管理

- 無論如何，您都不能僅基於同意權來處理所持有的資料，而忽視對 GDPR 的遵循性。
- 因此當組織是以取得當事人同意來作為處理個人資料的法源依據時，為確保其遵循性，組織應達到以下要求：

✓確保目前所取得的同意權皆符合 GDPR 規範，若否，便需重新取得資料主體的同意意向

✓確保所有的同意權都可以被立即呈現，若否，必須重新取得資料主體的同意意向，並且保留一份同意紀錄

✓必須確保敏感性資料已經額外取得同意（例如：醫療數據 / 健康數據 / 保險理賠資料等）

✓確保在資料蒐集以及隱私聲明的所有程序中，能清楚地向資料主體傳達撤銷同意權的流程

✓鑑別未成年人的資料主體相關資料（台灣為20歲，歐盟則為 16 歲），確保已經獲得其監護人的同意，若否，則必須重新取得其監護人的同意

bsi.

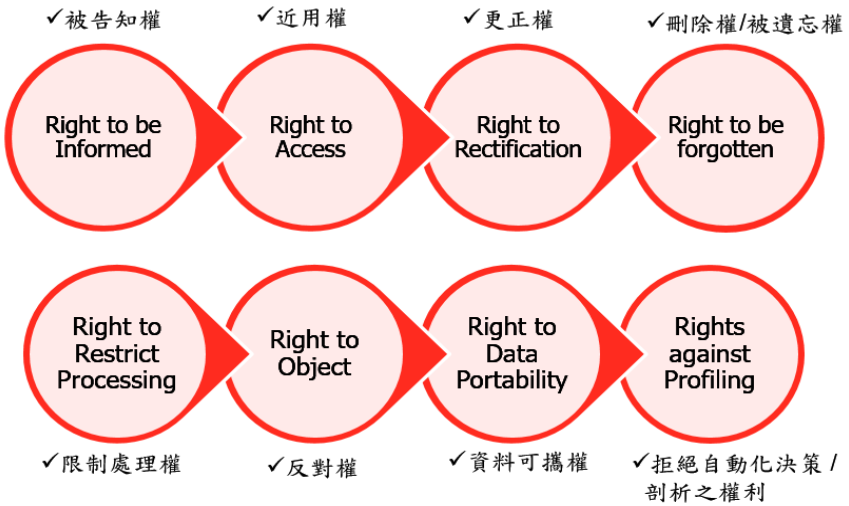
Step 8 - 資料留存

- 前述各步驟已協助我們對資料有新的認識，現在必須關注的是資料處理的原因，以及資料應留存的時限。
- 請審查您的盤點清冊、資料流程圖，以及任何過去曾經取得同意權，但已超過留存時限的資料，您現在必須以安全可靠地方式將其刪除、銷毀。

Step 9 - 資料主體權利 (治理面)

- GDPR 為一些既有的資料主體權利賦予更明確的定義， 並且增加了一些新的權利，組織將需要加以治理並採用技術方法，來建立能夠回應對 GDPR 遵循性需求的作業流程。
- 首先從治理的角度來看，組織應該同意並記錄治理政策和流程，以回應以下規範的要求:

Data Subjects Rights 資料主體八大權利



個人資料可攜權Data portability

GDPR使歐盟資料當事人能對自己的個資擁有更大的控制權，包括「資料可攜權」，也就是在不同服務之間移動個資的權利，用戶可以將其個人資料以及其他相關資料轉移。

(例: line聊天備份、Instagram資料備份)

刪除權/被遺忘權 (Right to be forgotten)

- 增加刪除權利，賦予個人可更有效的控制其個人資料。也被稱為「資料抹除」，可讓資料當事人要求資料控制者抹除其個人資料、停止使用個資，包括其供應商或其他第三方。
- 抹除條件可包括: 與處理目的不同、非法處理個資，或資料當事人撤銷同意書等，均可要求刪除。
- 歐洲法院過去已有判例裁定個人可以要求搜尋引擎從包括「不相關」或「過期」的個人資訊結果中移除連結。

反對權（Right to object）
/拒絕自動化決策 / 剖析之權利 (Rights against Profiling)

- 個人反對權係資料當事人有權，在特定情況下，反對資料之處理，除非資料控制者證明處理該資料有重大正當理由。
- 當資料當事人提出反對時，資料控制者應立即停止處理該個人資料。
- 亦適用於以大量個人資料所自動化產生之「剖析（profiling）」活動，資料當事人有權瞭解一項特定服務是如何做出特定決策的，此一規範將對以大數據為基礎，運用機器學習、人工智慧技術進行資料分析與研判的服務，將形成重大挑戰，機器學習技術很難適用「反對權」。

bsi.

Step 10 - 資料主體權利 (技術面)

- 從技術的層面而言，組織應當同意並記錄其使用的技術方法，以回應資料主體行使相關權利。
  - ✓ 資料主體近用要求
  - ✓ 限制處理 / 反對之權利
  - ✓ 更正權
  - ✓ 刪除權
  - ✓ 拒絕自動化決策 / 剖析之權利
  - ✓ 資料可攜權

Step 11 - 資料外洩的回應

- GDPR 資料外洩通報規範，即資料外洩發生時，必須在 72 小時之內，提報給資料保護主管機關（因而影響資料主體），若對資料當事人之權益有重大危害之虞，應未延遲 (without undue delay)(未明確規範期限)通知資料主體。
- 面對提報主管機關得在 72 小時的要求，即使在最佳的情況下也是非常具挑戰性的，如果沒有充份的理解， 並且定期檢測資料外洩的回應流程，組織可能幾乎無法達成這項責任義務。
- 組織必須同意並記錄資料外洩 / 資料安全意外事件的回應流程，並定期進行測試，以確保資料外洩事件發生時，這套流程可以切合需求。
- 進行資料外洩事件模擬演練，可以找出該流程之中的缺口，並且確保組織針對資料外洩事件已充分準備妥當，能做

如果個資外洩不太可能(unlikely)對資料當事人造成影響，沒有通報要求

Step 12 - 維持資料安全與防護

- 關注您正在處理的資料，以及與您共享資料的各單位。
- 審查您的盤點清冊、資料流程圖，以及任何組織所接收、分享或傳輸的資料，並審查相對應的安全規範。瞭解其中是否有任何潛在的安全顧慮，可能的話，請標示出需要審查與修補之處。最理想的情況，是組織可以透過內部的資訊安全相關單位，或外部顧問，來完成此這項工作。
- 所有存放資料的裝置及資料傳輸流程圖，都必須完成上述作業 (例如：靜態資料及動態資料)。

Step 13 - 隱私衝擊評估之基準

- 採取「隱私保護設計 (Privacy by Design)」或「隱私保護預設 (Privacy by Default) 」被認為是隱私保護工作的最佳實務做法，如今，GDPR 的最新規範已將之視為必須遵行的法定門檻。
- 組織現在需要進行資料隱私衝擊評估 (Data Privacy Impact Assessments, DPIAs)。
- 資料隱私衝擊評估是指，從風險管理的角度來審查資料處理活動的過程。實際上，這就是風險評鑑，目的是針對那些個人資料正在被處理的資料主體，審查其隱私風險的特性。
- BSI 建議訂定一項隱私權衝擊評估基準，目前所有已儲存或處理的資料，都應該予以審查，確保能夠找出任何潛在的隱私風險，以及可能的疑慮，並且呈報給管理階層審查。
- 執行這項可追溯的隱私衝擊評估作業，並非 GDPR 的強制規範。但當發生資料外洩事件，或是主管機關判定組織有不合規的事項時，若在調查後發現這些漏洞或流程缺陷，是在執行隱私衝擊評估作業時就能被發現的，則所受的罰款預期將可能更高。因此，完成隱私衝擊評估，將被視為此類狀況的自保對策。

bsi.

Step 14 - 隱私衝擊評估作業

- GDPR 的新規範之一是要求實施「隱私保護設計」與「隱私保護預設」機制，指的是隱私衝擊評估必須在以下兩種情境付諸施行：
  - 新蒐集或處理個人資料
  - 將組織既有的個人資料應用於新的用途或目的
- 當上述情況發生時，組織應採取具一致性、系統化及可重複進行的方法，以實施持續的隱私衝擊評估，並且同意予以記錄存檔。
- 從 BSI 豐富的稽核經驗來看，這可以透過在既有的作業流程中，增加控制項或觸發機制來達成，如：
  - 系統生命週期 (SDLC)
  - 專案管理
  - 變更管理

Step 15 - 管理階層的參與

- 由管理階層監管資料處理活動，一直被視為資料保護的最佳實務，但在 GDPR 頒佈後，這已成為最新的法令規範。
- 董事會或組織管理者高層，現在被要求展現對資料保護工作的參與，並且要掌握組織內部資料處理的狀況。
- 資料保護長必須將組織目前的資料保護概況，做為董事會會議的固定報告議題。
- 為了更適當地協助管理階層參與資料保護工作，協助他們瞭解當前的法令規範，資料保護長必須將相關的資訊與績效指標呈報給管理階層及董事會成員， 並取得共識。
- BSI 建議績效指標應該包括但不限於如下內容：

  ✓事件

  ✓未遂事件

  ✓資料主體權利行使要求

  ✓隱私風險監管 / 隱私衝擊評鑑之結果

  ✓與第三方分享的資料及遵循性監管計畫

Step 16 - 維護詳細的處理紀錄

- 如同 GDPR 第 30 條中所示，組織維護資料處理作業的詳細紀錄已是法定責任。
- 若組織能依循我們建議的順序，完成步驟 8 及 12 所提及的資料盤點及資料流程圖等作業，則組織應該已經符合此項規範的基本要求。
- 某些仍需要加以維護一些額外紀錄。BSI 建議處理紀錄至少含括如下內容：
  - ✓ 資訊紀錄
  - ✓ 資料留存紀錄
  - ✓ 第三方單位傳輸紀錄
  - ✓ 資料主體權利行使要求紀錄
  - ✓ 資料主體權利行使下之處理紀錄
  - ✓ 訴怨紀錄
  - ✓ 資料處理者監管紀錄，等 …

Step 17 - 教育訓練

- 讓員工認知到資料保護的重要性，對組織而言永遠都是最重要的。
- 依據 GDPR 的規定，組織將需要確保所有的員工，都已接受與其職能相對應的適當訓練。
- 在實務上，這意味組織內所有員工在到職之初，或至少每年，都應接受資料保護的相關訓練。
- 而對日常業務需要處理個人資料的關鍵員工，則被期許透過適切的訓練，獲得妥善保護資料的作法，這往往需要針對員工各別的業務性質，提供特定的訓練內容。

bsi.

Step 18 - 資料保護政策

- 從組織內部的觀點而言，組織必須重新界定目前的資料保護政策，以回應前述作業的產出成果。
- 組織的資料保護政策必須明確說明，其運作方式是如何符合 GDPR 的原則，並且為員工提供一份適當的資料保護指南。
- BSI 建議為符合透明化與明確性之義務，組織的資料保護政策也應該成為對員工的內部隱私聲明，該政策必須明確指出雇用期間對員工個人資料的處理
- （例如：員工的哪些個人資料被儲存或處理，以及原因為何，這些資料的留存期限，以及員工如何行使其資料主體權利等等）

bsi.

Step 19 - 隱私權聲明

- 從外部的觀點而言，組織必須重新界定目前的隱私權聲明，以回應前述作業之產出結果。
- 隱私權聲明應要能向您的顧客或第三方，明確地說明其資料被儲存或處理的作業性質與內容。
- 為符合 GDPR 要求之透明化與明確性的責任義務，組織的隱私權聲明必須在資料蒐集的每一個過程中都可以被取得（或至少可以查看參考），讓外部利害關係人能充分知曉：
  - ✓ 組織所擁有的資料
  - ✓ 擁有資料的原因
  - ✓ 資料經過哪些處理
  - ✓ 資料被儲存在哪裡
  - ✓ 資料被留存的時間
  - ✓ 資料主體所擁有的權利
  - ✓ 資料共享的對象
  - ✓ 如有隱私方面的疑問，可以諮詢的對象

Step 20 - 溝通

- 將更新過的資料保護政策與隱私聲明公開發布，並提供給所有相關的內 / 外部利害關係人。
- 所有相關的資料主體—包括內部與外部，現在都可以被視為已經獲知組織在資料保護的作法，以及如何行使資料主體的相關權利。
- 必須留意的是，這些資料保護透明化的工作，被預期將促使資料主體更積極的參與，組織將有可能接到更多來自資料主體的權利行使要求，或行使刪除權、限制處理權，或行使資料可攜權，結果可能導致行政管理上的更多負擔。
- 這些情況是可從 GDPR 的規範設計上所預期的。然而，假設已經適度採取本白皮書中所有的步驟，組織就應該無須過度[illegible]法將具有韌性，且能將任何潛在的風險減至最低。

...making excellence a habit.™