GDPR 實體安全性與隱私保護

歐盟的一般資料保護法規(以下簡稱GDPR)，要求全球的企業組織重新思考如何存取、使用以及維護個人資料。本白皮書介紹資料風險可能導致違反新法規的行政干預和經濟處罰。它也探討了實體安全與隱私的最佳實踐-因為他們代表了一個重要卻又常被忽略的資料保護領域。整合行政管理、網路安全與實體安全措施，可以協助保護敏感的個人資料，顯現企業組織對於資料隱私的重視。

關鍵要點:

- 了解GDPR關於保護個人資料的實體安全與隱私措施。
- 探索何謂專家所認為的資料保護與隱私的合理水準。

生活在資料驅使的世界

大多數的企業組織收集與使用個人資料，作為當今商業行為的一部分，無論是人事、客戶、潛在客戶或是第三方的。典型情況下，這些資料是以電子形式儲存，提供企業組織[1]與外部各方存取。此外，一些企業組織的主要功能是收集與分析大量的個人資料。

雖然每個企業組織所收集的資料量和類型各不相同，但是人們普遍認為搜尋這些資料從未如此的簡單。民眾在建立社交媒體檔案、參與線上社交、進行網路搜尋、回答問卷以及索取促銷優惠與“免費”服務(例如照片儲存和串流音樂服務)時會留下一長串的資料。

隨著人工智慧、電子標籤、網路信標、小型文字檔案(cookies)，以及其他監控工具的進步，科技協助了人們建立健全的個人資料。

科技與資料探勘的結合，使得企業組織能夠累積珍貴的個人資料。這些儲存庫可以揭露一個人的年齡、婚姻狀況、生日、教育程度、嗜好、宗教信仰、工作經歷、政治信仰、購物習慣、新聞來源偏好、收入、犯罪背景等等。

儘管這些資料大都集中在公司的資料庫中，仍有部份資料分散在整個供應鏈內的不同系統中，往往缺乏對未來的接受方傳達這些最初的資料是如何或是為何收集的機制。這將使得個人資料的使用偏離當初收集時的目的。

每天，企業組織內的許多人都可以使用儲存的資料—可能是支付薪水、進行市調、舉辦電郵行銷或是追蹤客戶的參與度。這些資料庫的使用，代表著個人資料被濫用或是落入不法之徒的機會。

重點摘要

什麼是GDPR?

一般資料保護法規(GDPR)，旨在保護歐盟民眾的隱私。

何時生效?

2018年5月25日

誰會受影響?

所有控制或處理歐盟民眾個人資料的公司，無論公司位於哪一個國家或地區。

什麼構成了個人資料?

任何與自然人或資料當事人有關的資訊。它可以是名稱、照片、電子郵件地址、銀行細項、社交網站上的貼文、醫療資訊或是電腦的IP位址。

會有什麼影響?

罰款2,000萬歐元，或是全球年營業額的4%(以較高者為主)。這是對最嚴重的侵權行為所處的最高罰款。

我可以在哪裡取得更多的訊息?

- 法規概述
- 閱讀法規
- 實體安全解決方案

想了解更多?

請至 3m.com.tw/3M/zh_TW/privacy-screen-protectors-tw/

65%

的受訪者表示，資安外洩確實使他們失去對企業組織的信任。[5]

要了解企業組織面臨的實體安全風險，請參考以下情節:

員工在機場查看手機裡的敏感資料，卻沒有察覺到附近有人正注視著他們的螢幕。

- 員工遺失了筆電，而硬碟上的資料並未加密。
- 員工離開辦公桌去倒咖啡，將客戶的聯絡訊息留在螢幕上或是桌上，剛好有未經授權的人員經過。
- 不滿公司的員工對著留在印表機上的文件、螢幕上的資訊以及貼在電腦螢幕上的登錄憑證拍照。
- 將過時的筆電或是桌電捐贈給慈善機構，卻沒有完全清除硬碟裡的資料。
- 醫生辦公室人員將無用的病患資料丟棄到垃圾桶而沒有撕碎。

在 2016 年，駭客共入侵了

10 億條記錄[2]

像這樣的情節越來越令人擔憂，資安外洩事件在現今數位化世界太常見了。Forrester報告說，光2016年，駭客就入侵了10億條記錄。據統計，2017年上半年有918起的資料外洩事件，導致全球有19億條資料受到威脅。與2016年上半年相比，增加了164%。[2]

隨著每一次新的資料入侵出現，資安隱私的消逝就會令人越感焦慮。根據最近的一項研究指出，人們感覺到他們的隱私正受到安全性與保密問題的威脅。事實上，91%的人擔心自己已經無法掌控企業如何收集與使用他們的個人資料。而幾乎相同數量的人認為，要在網路上移除有關他們自己的不正確訊息是非常困難的。[3] 不僅僅是大型違規需要擔心，小型企業可能持有較少的個人資料，但是如果被盜用或是濫用，對當事人而言仍是一樣的嚴重。

即便嚴格的資料隱私以及資料保護指令和法規已經存在十多年了，這些擔憂仍然持續著。美國的健康保險可攜性及責性法案(HIPAA)、公平信用報告法以及歐盟的資料保護指令就是明顯的例子。

資料保護指令，概述了一些原則，例如處理資料要講求安全性，限制其使用目的，並且不長時間保存。然而，它只是一項“指令”而非法律，歐洲各國的執行力與強制力是不一樣的。

了解GDPR

GDPR是為了保護個人資料而導入的最全面以及最具全球影響力的法規。它的創立是為了一個共同的信念，就是人人都有基本的隱私權。它旨在保護歐盟民眾的個人隱私，其手段是透過實行新的法規來監管企業如何保護、處理和使用個人資料。

GDPR也許是近20年來，在資料安全與隱私監管方面最重要的進步--因為它對資料記錄的問責要求，以及它潛在的財務影響。透過兩級制罰款，企業組織可能會因為違反以下情形而被罰款2%的全球年營業額或是1,000萬歐元，例如:

- 未能向監督當局與受影響的當事人告知有關資料外洩事宜。
- 當企業組織有需要時，未能任命資料保護官(DPO)。

企業組織可能被罰款4%的全球年營業額或是2,000萬歐元，例如:

- 不尊重資料主體權
- 不遵守監督機構的命令
- 不遵守國際資料傳輸的規定[4]

這些罰款除了會損害商譽、品牌價值與信任之外，對公司的淨利也同樣具有破壞性。事實上，資料外洩事件會讓65%的民眾對該企業組織失去信任。[5]

要符合GDPR規範是一項不小的工程，因為它要求企業組織負起收集、使用、維護和清除個人資料的責任，同時保證其安全。即使是公司現有的隱私與安全性計畫，都需要重新評估其流程。具體來說，GDPR要求企業組織採取適當的技術與組織安全性措施來防止個人資料的遺失或是未經授權的存取。

GDPR 是為了保護個人資料而導入之最全面和最具全球影響力的法規。[1]

這裡有一些問答:

問: 什麼構成了個人資料?
答: 任何與已辨識或可辨識之自然人有關的訊息。這可能包括標識符(例如姓名或身分證號碼)或是揭示種族或族裔出身的資料，政治觀點、宗教或是哲學信仰、工會會員資格、基因資料、健康資訊、刑事犯罪、工作績效預測、經濟情況、個人喜好或興趣、可靠性或行為、位置或行動等等。[7]

問: 什麼是虛擬假名? 為何我應該注意?
答: 這個術語“虛擬假名”(pseudonymization) 在GDPR中被提到15次之多，它是指在一個資料記錄中的識別字段，被一個或是多個人為的標識符或是化名所代替的程序。GDPR建議使用虛擬假名建立個人資料以降低資料主體的風險，並協助控制者與處理者履行資料保護的義務。[8]

問: 企業組織是否可以取得民眾同意來收集他們的個人資料?
答: 可以，但是此同意需要透過明確的、肯定的行為來給予，而該行為是自由地提供、明確的、知情的、不含糊的指令來表示資料主體(當事人)同意處理其個人資料。預先打勾、拒答、或是非使用狀態，皆不構成同意。企業組織需要維護接收資料主體同意的記錄，並使用清晰明瞭的用詞，確保請求資料主體同意與其他的請求區分開來。[10]第13條概述了在收集個人資料時，需要向資料主體提供詳細的訊息，例如收集資料的目的、個人資料的接收方或是接收方的類別，以及資料儲存的時間長度。

問: 什麼是資料保護影響評估(DPIA)?
答: 高風險活動所需的DPIA，有助於企業組織評估風險的來源、性質、特殊性與嚴重性，並採取適當的措施來降低風險，例如加密。在評估資料安全風險時，應考慮到傳輸、儲存或其他方式處理個人資料時所帶來的風險，例如意外或非法破壞、遺失、變更、未經授權披露或存取，可能導致實體、物質或非物質的損害。[11]

問: 我需要指派一位資料保護官(DPO)嗎?
答: 公共部門(法院以司法身分行事除外)進行資料處理，或是公司的核心業務是需要對資料主體進行大規模定期且系統性的監控處理時，指派DPO是必要的。所有處理大量敏感資料(例如健康、宗教或政治信仰)的企業也是必須指派DPO。具體而言，DPO:

- 必須根據其專業素質，特別是關於資料保護法及慣例的專業知識來任命
- 可以是公司員工或是委外服務人員
- 其連絡方式必須提供給相關的資料保護局(DPA)
- 必須被賦予適當的資源來執行任務，並保持其專業知識
- 必須直接向最高管理階層報告
- 不得執行可能導致利益衝突的其他任務[12]

實體安全與隱私要求
企業組織應該做什麼來防止資料外洩?GDPR第24條概述了企業組織有責任去執行“適當的技術與組織安全性措施”，以確保並展示正確的個人資料處理。第32條則是進一步解釋到: “在評估適當的安全級別時，應考慮到傳輸、儲存或其他方式處理個人資料所遭遇之風險，特別是來自於意外或非法破壞、遺失、變更、擅自披露或存取時”。

此法規的一個重要面向是強調防止未經授權的存取。這是實體安全必不可少的地方。具體來說，它可以協助保護資料免受內部和外部人為威脅的影響，這些威脅會利用企業組織內部部門之間以及員工間的漏洞來達到目的。這包括限制可以被觀察、竊取或存取的資料。請審視以下內容，並評估您的員工是否有適當的技術與組織安全性措施。

以設計與預設來配置資料保護:

為了保護資料，企業組織必須主動識別和收集其預定用途所需之個人資料，只在必要時間內保留資料(最小化原則)，並確保個人資料不會被無限數量的人數所存取。這可能涉及到確保隱私風險被預先確認，而系統旨在減輕這些風險；適當地使用虛擬假名和匿名、在處理功能中創建透明度，以及確認需要存取資料的特定人員或身分。問問您自己: 在設計資料系統、商業慣例和實體設計之前，您是否有考慮到個人隱私風險? 您是否有跟您的IT人員審查當前的系統與處理工作，並討論是否需要採取額外的步驟來記錄在整個資訊生命週期中如何保護個人資料?

使用實體保護措施:

網路安全控制(例如資料加密和複雜的密碼)至關重要，而"低科技"管理與實體控制同等重要。要決定哪裡需要實體屏障，請確認存取敏感資訊的位置。例如，員工經常使用行動裝置從任何地方來存取和共享資料。越來越多這樣的員工在公共場所存取敏感資訊，往往在眾目睽睽之下。辦公室內的資料暴露風險也增加了，常見的開放式辦公室規劃移除了原本可以遮蔽電腦螢幕的實體屏障。問問您自己: 您有將電腦螢幕放置在可被公開造訪的窗戶、門和區域之外嗎? 您是否有在顯示器以及手機螢幕安裝隱私防窺片來阻擋潛在的旁觀者觀看上面的資訊? 共享的印表機/影印機/傳真機有放在受保護的區域還是有鎖上蓋子? 您是否將資料的實體副本放在有存取管控的設備中? 碎紙機是否是所有現場設備(特別是影印機、印表機和傳真機)的標準配備? 且是所有遠距工作者或是使用遠端存取公司訊息資產者的必要設備?

安排員工培訓

培訓計畫應涵蓋三個主要面向: 觀察、實體存取、防盜之最佳實踐。例如，當員工在公共場所使用筆電、平板電腦和手機來存取與管理遠端連結的設備時，應提醒員工注意周遭環境。設備螢幕不應該暴露給路人和潛在的旁觀者，尤其是在輸入登錄資訊或是查看敏感帳戶的詳細資料時。而在實體存取方面，企業組織應該訓練員工在開完會後清除白板上的資訊和回收機密文件；記住密碼而不是抄寫下來；將文件櫃與筆電上鎖；在電腦螢幕上安裝隱私防窺片；保持桌面清潔，包括登出無人看管的設備。問問您自己: 您的培訓計畫是否包含情境意識，以便員工學會注意周遭環境，並能夠辨識和回應可疑的行為? 員工是否了解企業組織對"乾淨的辦公桌"政策的期望? 您是否經常提醒員工必須遵守良好的安全措施?

制定明確的政策:

為了表明企業組織對實施適當的安全與隱私措施的承諾，其政策便應該讓員工與承包商了解在工作場所和遠端工作使用與查看資訊的規範。員工協議應包含有關保護敏感與機密資訊責任的具體措辭。[13] 問問您自己: 您是否有向民眾傳達貴公司如何保護、共享、處理個人資料以及提供個人資料的存取? 您是否有BYOD(自帶設備)政策來管理員工的行為，並在他們從個人設備存取竊業資源時採取必要的安全管控措施? 作為安全政策的一部分，您是否要求員工同時使用視覺與網路安全控制?

設置資料儲存限制:

根據適用的法律，設定個人資料儲存時間的長短。安全地清除所有並非絕對需要的個人資料，以支持收集個人資料的業務目的。問問您自己: 您有什麼樣的技術控制可以在正確的時間消除資料? 貴公司的銷毀流程是否符合如NIST特別出版物800-88所提供之強大的安全性指導方針，例如實體銷毀已達壽命期限的硬碟?

想了解更多?
請至 3m.com.tw/3M/zh_TW/privacy-screen-protectors-tw/

螢幕防窺
專家

3M Science. Applied to Life.™

驗證第三方供應商:
只使用能夠提供足夠專業知識、可靠性和資源保證的處理人員來執行技術與組織安全性措施，包括處理的安全性。問問您自己：您是否有供應商管理計畫，包括合同義務，並可以為存取個人資料的第三方建立管理監督工作?

創建資料洩露協議:
企業組織必須做好準備，在知道發生個人資料外洩(如果可行，最遲不超過72小時)的情況下，通知監管機構，不得有不當的拖延。或者，能夠證明個人資料外洩不會對自然人的權利與自由造成風險。如果存在高風險，資料主體(當事人)也必須被通知資料外洩，不得有不當的拖延。(14) 問問您自己：您上一次是在什麼時候審視貴公司的事件應變與外洩通知的政策與計畫? 員工的設備若是遭到入侵，或者意識到資料外洩，他們是否知道該向企業組織內的何者告知? 您是否有最新的事件應變與外洩通知的計畫，以便決定何時以及如何向主管部門通報資料外洩?

了解個人的權利:
歐盟居民現在有權查看企業組織手上有關他們的個人資料，並可以在某些情況下要求刪除其資料。刪除權能要求企業組織刪除跟這些個人資料的相關的任何連結、拷貝或複製。企業組織應該提供人們以電子方式提出請求，尤其是在透過電子手段處理個人資料的情況下。(15) 問問您自己：貴公司是否了解什麼被視為是"個人資料"，以及如何回應有關個人資料的查詢?

結論:

GDPR是20年來資料隱私監管方面最重要的變化。它要求個人資料的管理方式可以有助於確保適當的安全性和保密性—這是一項需要技術與組織安全性措施的任務。公司因為不合規而遭受的罰款可能影響巨大。但是，法規中概述的最佳實踐就是做良好的生意。沒有人希望他們的資訊被濫用，沒有企業組織希望面對資料外洩的後遺症。企業組織不將隱私視為合規的負擔，而將其視為企業責任的戰略策略，能提高其商譽和品牌價值、吸引更好的員工，以及最終能維持公眾的信任。

想了解更多?請至 3m.com.tw/3M/zh_TW/privacy-screen-protectors-tw/

(1) Forrester，從世界上最大的安全漏洞和資料濫用中吸取的教訓，2017年1月9日
(2) 2017 Gemalto 違規指數，http://www.gemalto.com/press/Pages/First-Half-2017-Breach-Level-Index-Report-Identity-Theft-and-Poor-Internal-Security-Practices-Take-a-Toll.aspx
(3) GfK Privacy Panel，後史諾登時代公眾對隱私和安全性的看法，2014。
(4) 第83條，the GDPR，2017
(5) Ponemon Institute，資料外洩對聲譽和共享價值的影響，由Centrify贊助，2017。
(6) 第4條，the GDPR，2017
(7) 第75號，the GDPR,，2017
(8) 第26號與28號，the GDPR，2017
(9) 第32號，the GDPR，2017
(10) 第7條，the GDPR，2017
(11) 第35條與第83-84號，the GDPR，2017
(12) 第37-38條，the GDPR，2017
(13) 第74、77-78號，the GDPR，2017
(14) 第81號，the GDPR，2017
(15) 第59、63、65、66號，the GDPR，2017