臺北市政府法務局資料治理暨個資保護研討會

我國及GDPR資料外洩規範與案例分析

- 世新大學法律學院
- 戴豪君
- 2022.09.26
- irving@mail.shu.edu.tw

世新大學
Shih Hsin University

報告大綱

- 前言
- 個資法消費者資料外洩規範與案例
- GDPR資料外洩規範與案例
- 結語

前言：個資外洩案件層出不窮

- 根據刑事警察局統計2021年全年前5大高風險賣場名單，分別是誠品書店、東森購物、蝦皮購物、婕洛妮絲、金石堂

資料來源：https://www.ithome.com.tw/news/149057

前言：個資外洩案件層出不窮

■ 知名電商平台會員個資外洩，導致民眾被詐騙而報案及諮詢件數達九百餘件

資料來源：https://udn.com/news/story/7320/6015536

資料來源：刑事警察局公共關係室

個資法消費者資料外洩規範與案例

個資外洩通報實例（一）

BBC Sign in | Home | News | Sport | Reel | Worklife | Travel | Future | Culture | More | Search

NEWS

Home | Coronavirus | Video | World | Asia | UK | Business | Tech | Science | Stories | Entertainment & Arts | More

Business | Market Data | New Economy | New Tech Economy | Companies | Entrepreneurship | Technology of Business | Business of Sport | Global Education | Economy | Global Car Industry

McDonald's hit by data breach in Taiwan and South Korea

11 June

Top Stories

Ethiopian rebels gain more ground in war-torn north

Tigrayan fighters continue their advance after wresting the regional capital from government forces.

43 minutes ago

Hong Kong's year under a controversial security law

1 hour ago

Chinese students 'fear speaking out' in Australia

11 hours ago

資料來源： https://ww.bbc.com/news/business-57447404w

站內搜尋 | 高島屋 (重新選擇)

別具滋味 | 企業永續 | 數位便利 | 現正推出 | 尋找餐廳

公告

本公司頃接獲麥當勞總部通知，知悉有未經授權之第三方侵入麥當勞全球網路系統竊取資料，包含麥當勞歡樂送的台灣與南韓部份資料及台灣少數人事及部分管理資料，目前已知歡樂送訂餐資料中含有個人資料包括EMAIL、聯絡電話及送餐地址但不含任何財務資料 (如銀行帳號、信用卡卡號及密碼)。針對此一資安事件，本公司除立即與麥當勞總部共同進行資安檢查，提高網站的資安防禦，包括身份認證管理、終端設備防禦以及資安監控外，並就此起網路犯罪事件已通報相關司法及行政機關。本公司對本事件致受影響之人，謹表達最誠摯的歉意。

本公司一向重視顧客服務與個人資料保護，從未以任何方式蒐集顧客的銀行帳號、信用卡卡號及密碼；由於遭竊取的檔案不含顧客財務資訊，評估一旦外洩的主要風險，恐為收到垃圾郵件、不明簡訊或成為詐騙對象。

為求慎重，本公司特此公告，並將陸續以適當方式通知受影響之人。若接獲自稱台灣麥當勞客服人員或任何不明第三人，來電詢問個人財務資訊，務請提高警覺避免受騙。如有任何疑問，請利用本公司官網客服信箱提供協助。https://mcdonalds.ptcnec.com.tw/contact/index (2021/6/11)

敬請點選連結，查詢您於歡樂送登錄之 EMAIL 帳號是否受到第三方侵入。
點此進入查詢頁面：https://announcement.mcdonalds.tw

資料來源： https://www.mcdonalds.com/tw/zh-tw/post/20210120.html

個資外洩通報實例（二）

首頁 > 資訊安全 > 陽明校區疑似個資外洩通知

陽明校區疑似個資外洩通知

2021-05-31 • 資訊安全

本校陽明校區於110年1月7日發現駭客利用活動報名系統的弱點，疑似竊取本校教職員工(含離職人員)個資約1萬筆，本校依個人資料保護法第12條及施行細則第22條規定通知當事人相關事項如下：

一、影響範圍：陽明校區自99年導入資訊系統時，活動報名系統連結教職員工資料之共用表，實際影響人數為 10,008人，個人資料包含：員工編號、姓名、身分證號、職稱、Email、電話、地址等資訊。
二、因部分離職教職員無聯繫方式，本校無法一一通知，若您對於您的個人資料有所疑慮請洽承辦人。
三、本校已調整系統架構，加強資訊安全的防護，並依資通安全管理法向教育部進行資安事件通報。

為了避免您遭受損失，請您提高警覺慎防詐騙。

針對本事件，本校將確實檢討改進，並依資通安全管理法及個人資料保護法持續精進各項資通安全及個資保護相關作為。

承辦人：

- 聯絡電話：
- Email：lcy[redacted].edu.tw

資料來源：https://it.nycu.edu.tw/news/6808/

個資法個資外洩通知義務(一)

- 通知當事人義務(§12)
  - 公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
  - 施行細則第22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。

什麼叫做？

個資法個資外洩通知義務(二)

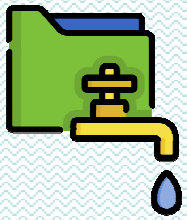
- **個資法施行細則第22條第2項所稱「個人資料被侵害之事實」及「已採取之因應措施」**(法務部105年4月20日法制字第10502506140號函)
  - 「個人資料被侵害之事實」及「已採取之因應措施」應包括：個資外洩之事實、業者所採取之因應措施及所提供之諮詢服務專線。又上開規定未限制公務機關或非公務機關提供與個資侵害事故有關之其他訊息（不包含與個資侵害無涉之資訊，例如行銷廣告）
  - 建議公務機關或非公務機關於適當時，宜併提供當事人應採取措施之具體建議（例如重新設定密碼、聯繫銀行及信用卡發行公司、警戒可能之詐騙行為），以防止損害之發生或擴大。

個資外洩通知相關法規義務（1/6）

■ 個資外洩與資通安全管理法通報義務

- 資通安全管理法第14條規定公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報主管機關；無上級機關者，應通報主管機關。
- 依資通安全事件通報及應變辦法立法說明將所稱「敏感資訊」，指包含個人資料等非一般公務機密或國家機密之資訊，如遭洩漏可能造成機關本身或他人之損害或困擾，而具保護價值之資訊。個資外洩可能構成依同辦法第2條規定資通安全事件。依同辦法第6條規定：公務機關在知悉資通安全事件發生，應於該事件一定期間內。完成損害控制或復原作業，並依主管機關指定之方式及對象辦理通知事宜。

■ 上市公司個資外洩



- 可能屬證券交易法第157條之1第5項所稱涉及該證券之市場供求，對其股票價格有重大影響，或對正當投資人之投資決定有重要影響之消息，需依規定通報證交所

個資外洩通知相關法規義務（2/6）

■ 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計畫實施辦法

- 本辦法於110年12月8日修正公布：課與學校、機構應自資安事故發現時起72小時內，通報主管機關之義務
- 本辦法第8條規定學校、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。應變機制包括：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
- 學校、機構應自事故發現時起72小時內，填具個人資料侵害事故通報與紀錄表，通報主管機關，未依時限內通報者，應附理由說明；並自處理結束之日起一個月內，將處理方式及結果，報主管機關備查

個資外洩通知相關法規義務（3/6）

教育機構資安通報平台

資料來源： https://info.cert.tanet.edu.tw/prog/index.php

個人資料侵害事故通報與紀錄表

第八條附件

個人資料侵害事故通報與紀錄表		
非公務機關名稱 通報機關	通報時間：　年　月　日　時　分 通報人：　簽名（核章） 職稱： 電話： E-mail： 地址：	
事故發現時間		
事故發生種類	□竊取 □洩漏 □竄改 □毀損 □滅失 □其他侵害事故	個資侵害之總筆數（大約） □一般個資＿＿＿＿筆 □特種個資＿＿＿＿筆
發生原因及事故摘要		
損害狀況		
個資侵害可能結果		
擬採取之因應措施		
擬採通知當事人之時間及方式		
是否於發現個資外洩後72小時通報	□是　□否，理由：	

個資外洩通知相關法規義務（4/6）

- **製造業及技術服務業個人資料檔案安全維護管理辦法**（110年12月30日修正公布）
  - 保有消費者個人資料之製造業及技術服務業達五千筆之業者，應依本辦法規定，規劃、訂定、修正與執行消費者個人資料檔案安全維護計畫
  - 所稱消費者，指以消費為目的而為交易、使用商品或接受服務者
  - 業者發生消費者個人資料安全事故（個人資料被竊取、竄改、毀損、滅失或洩漏），將危及其正常營運或大量當事人權益者，應於知悉事故後七十二小時內通報經濟部，或通報直轄市、縣（市）政府時副知經濟部。
  - 通報內容依該辦法附表二規定包括：事件發生種類、外洩大略筆數、發生原因及事件摘要、採取的因應措施、通知當事人的時間和方法。
  - 無法於時限內通報或無法於當次提供前項所述事項之全部資訊者，應檢附延遲理由或分階段提供。

個資外洩通知相關法規義務（5/6）

■ 資訊服務業者落實個人資料保護暨資訊安全參考指引

- 2022年4月經濟部工業局考量網路購物、網路訂房等電子商務服務蓬勃發展，消費者、會員個人資料外洩等資訊安全事件層出不窮。資訊服務業蒐集、處理或利用的個人資料數量龐大，個資侵害風險高於其他產業。受客戶委託建置網站前後台系統的資訊服務業者，更需強化其資訊安全防護措施及個人資料保護安全維護措施，特公布此指引。
- 通知當事人應由與消費者直接接觸、蒐集消費者個資之業者（例如電商業者、私人醫院診所、私立學校、非營利組織等），依個人資料保護法為通知。
- 系統商與其客戶基於契約關係，協助客戶代管主機或儲存資料時，因而保有消費者個資，因此當知悉消費者個資因資安事故有外洩等情形時，應立即通知客戶業者，並可基於與客戶的契約關係，協助代為通知消費者，提醒客戶業者通報其主管機關，終仍應由客戶業者自行負責

個資外洩通知相關法規義務（6/6）

- **網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法**（110年12月30日修正公布）
  - 網際網路零售業，指以網際網路方式零售商品。網際網路零售服務平台業，指經營供他人零售商品之網際網路平台。兩者登記資本額新臺幣一千萬元以上股份有限公司，或受經濟部指定之公司或商號。但不包括應經特許、許可或受專門管理法令規範之行業
  - 發生重大事故（指個人資料遭竊取、竄改、毀損、滅失或洩漏，將危及網際網路零售業正常營運或大量當事人權益）時，應自發現事故時起算七十二小時內，依附表格式，以電子郵件方式通報總機構所在地直轄市或縣（市）主管機關及副知經濟部
  - 因應措施包括：降低、控制事故對當事人造成損害之作法；適時以電子郵件、簡訊、電話或其他便利當事人知悉之適當方式，通知當事人事故之發生與處理情形，及後續供當事人查詢之專線與其他查詢管道；避免類似事故再次發生之矯正及預防機制

個人資料與消費者保護之關係（一）

- 法務部法律決字第10300211540號函
  - 消費者保護法規定應採取之消費生活發展所必要之消費者保護措施，包含涉及消費關係之個人資料保護：考量人民對個人資料保護事項之陳情案件，一部分係非公務機關對消費者個人資料蒐集、處理或利用所生之爭議，與消費關係有關，亦屬依消費者保護法第 3 條第 1項第 13 款之消費生活之發展所必要之消費者保護措施
  - 查消費關係爭議涉及個人資料保護之情形，建議由現行各地方政府消費者保護專責單位擔任處理之，並由行政院消費者保護處監督以保護消費者權利
- 個人資料與消保法之關係
  - 個人資料本身應不宜視為以消費為目的而為交易、使用之商品或服務

個人資料與消費者保護之關係（二）

■ 個人資料與消保法之關係

- 歐盟數位內容與數位服務供應契約指令(Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services)涵蓋電腦程式、應用程式、影像檔案、音訊檔案、音樂檔案、數位遊戲、電子書或其他電子出版，以及允許以數位形式創造、處理、接取或儲存資料之數位服務(包括軟體即服務，softer-as-a-service)，如：影像或音訊共享，與其他雲端運算環境與社群媒體中之檔案託管、文字處理或遊戲等。
- 適用於一次性或持續性的數位內容與服務。前者如電子書，後者如雲端儲存與社群媒體服務。包括有償（利用貨幣、電子票據、虛擬貨幣與個人資料）無償方式提供，但排除包含數位要素商品（goods with digital elements）如智慧型手機

個人資料與消費者保護之關係（三）

■ 我國個人資料與消保法之關係

- ➢ 電子商務消費者保護綱領
  - 告知、蒐集及使用限制、參與、資料保護等，確保消費者享有選擇權，並提供合理之安全保護措施
  - 設計開發行動及線上付款系統時，應納入隱私保護機制，並適時檢討、更新及整合現有機制
- ➢ 企業產生個人資料相關之消費爭議應考量下列規定：
  - 消保法第7條：從事設計、生產、製造商品或提供服務之企業經營者，於提供商品流通進入市場，或提供服務時，應確保該商品或服務，符合當時科技或專業水準可合理期待之安全性。
  - 消保法第12條定型化契約中之條款違反誠信原則，對消費者顯失公平者，無效。
  - 零售業等網路交易定型化契約應記載事項第十一點：企業經營者應遵守個人資料保護相關法令規定。

個人資料外洩之民事判決（1/4）

■ 個資外洩後續詐騙損失之因果關係採否定見解（台灣士林地方法院民事簡易判決106年度湖簡字第1147號）

- 被告公司之電腦遭駭客入侵，約有36萬餘筆客戶資訊遭竊事件，經見載於報紙、網路媒體，業經認定於前，則原告自應有所警覺與注意。又詐騙集團利用電話詐騙民眾前往ATM操作，此一再為政府、各媒體所宣導，原告應有防騙意識。被告已用簡訊通知採取適當避免原告因被告公司電腦遭駭客入侵 、客戶資料外洩，而可能遭受財產上損害之防護行為。
- 系爭ATM操作行為，致受有系爭財產上損害，當屬原告個人疏忽行為所致，難認該損害與被告未善盡對客戶個人資料之保護行為間，確有相當因果關係存在，即難該當上述侵權行為之法定要件。

■ 中斷個資外洩與財產上損害間因果關係（臺灣士林地方法院民事簡易判決109年度湖簡字第1959號）

- 考量詐騙集團介入行為對損害結果之強度，遠超乎原先個人資料外洩之影響，且屬故意犯罪行為，被告亦無防止該第三人不法行為之契約或法令上義務，堪認詐騙集團對原告施以詐術之故意行為業已中斷被告過失使資料外洩結果與原告財產上損害間之因果關係

個人資料外洩之民事判決（2/4）

■ 個資外洩與客戶因而受詐騙之損失具因果關係（臺灣士林地方法院民事判決107年度簡上字第225號）

- 2017年4月當事人張女使用手機登入EZ訂網站，購買2張電影票，後接到假冒EZ訂的會計人員的電話，核對張女的姓名、電話，以及購票日、場次與金額，謊稱作業人員疏失，誤植20筆原告之訂票紀錄（約8,000元），誆稱需要張女協助授權才能向銀行退費，張女被詐騙25萬。
- 富爾特公司為上市公司，藉由系爭網路平台留存消費者個人資訊以獲取利益，卻未就消費者之個人資料善盡適當安全維護措施，致洩漏張女個人資料而為詐騙集團不法取得使用，侵張女之資訊自主權、隱私權。…認張女請求富爾特公司賠償非財產上損害2 萬元，尚屬相當。
- 查富爾特公司確有洩漏其保有張女之個人資料若非詐騙集團取得張女留存於網站平台之個人資料，並使用該等明確、特定之個人資料以取信於張女，應不致於陷於錯誤而遭詐騙，堪認富爾特公司前揭未盡適當安全維護措施，致洩漏個人資料之行為，與張女遭詐騙受有25萬7,892元損害間有相當因果關係，自得請求該部分財產上損害之賠償

個人資料外洩之民事判決（3/4）

■ 當事人向企業與網站維運外包廠商以雇傭關係連帶求償（臺灣雲林地方法院民事判決108年度六簡字第198號）

- 江姓藝人於107年大同醬油公司網站訂購醬油2 瓶，後續發現其個人資料於搜尋引擎中輸入關鍵字搜尋，能取得原告完整個人資料，嗣經被告喬義司公司於得知該事件後即修復系爭網站等情，為兩造所不爭執，足徵原告個人資料遭外洩僅為單一事件。又原告未能舉證證明其因被告喬義司公司網站管理之疏失行為造成其受有50萬元損害之依據為何。自應回歸個資法第29條第2 項準用第28條第3 項規定，以每一事件500 元以上2 萬元以下酌定賠償數額
- 被告丙〇〇之行為既構成民法第184條之侵權行為，復係以擔任被告喬義司公司之專案經理職務時，對被告大同醬油公司網站取得之客戶資料未建置有效防護措施，致侵害原告之隱私權，故原告請求被告喬義司公司應依民法第188條第1 項規負僱用人責任，即與被告丙〇〇連帶賠償其所受損害，應予准許。

個人資料外洩之民事判決（4/4）

■ 負擔損害賠償之企業向網站維運外包廠商進行求償（臺北地方法院108年度訴字第1721號民事判決）

- 本件原告所取得者並非僅有旗艦版平台，亦包含網址服務、電子發票服務項目、SSL加密憑證、SSL憑證檔嵌入服務、其他系統串接維護費、物流系統串接維護費、系統串接維護費等多項加值服務，是原告所欲取得之標的，係具備上開功能與服務之電子商務網站，而非僅單純地租用網路平台。張系爭主契約及107年5月報價單為承攬契約。被告則抗辯駭客攻擊係屬不可歸責於己之事由所致等語。按兩造間成立承攬契約，被告既抗辯損害之發生係不可歸責於己之事由所致，自應由被告負舉證之責
- 被告辯稱其使用至少十數項資安防護措施，且創設數道繁複的手續，然被告所提供之網路平台在2年間即發生數次個人資料因駭客攻擊而外洩之事件，若真如被告所言採取國際公司規則之資安防護技術，應不致發生如此多次數駭客入侵之情形，惟被告所提供之網站若符合現行科技水準，依OWASP標準檢測之結果，其所獲得之評價亦不應落入最低等級之列，故難謂被告所提供之網站平台符合現行科技水準
- 原告請求解除契約後之報酬返還及損害賠償，包括返還報酬、個資外洩賠償第三人和解金，商譽損失共約102萬

GDPR資料外洩規範與案例

GDPR資料侵害通知之要件或義務（一）

■ GDPR資料侵害之定義（Art.4(12)）

- 個人資料侵害(Personal data breach)，係指違反安全性導致傳輸、儲存或以其他方式處理之個人資料遭意外或非法破壞(unlawful destruction)、遺失、變更、未經授權之揭露(unauthorised disclosure)或接近使用

■ 向主管機關通報義務（Art.33）

- 如因伺服器攻擊，導致保管在自己公司伺服器上的位於EEA的人其個人資料遭到洩漏之情形等。
- 個人資料侵害發生時，控管者即應依第 55 條向監管機關通報（Notification ）不得無故遲延，且如可能，應於發現後 72 小時內通報，但個人資料侵害未造成對當事人權利及自由之風險時，不在此限
- 如果沒有在72小時以內通報主管機關的話，也必須通報與遲延相關的理由。。

GDPR資料侵害通知之要件或義務（二）

■ 資料侵害之必要通報（通知）內容（Art.33）

- 描述關於個人資料受到侵害之性質，如果可行的話，相關當事人的種類以及大概數量。包括相關的個人資料之記錄種類以及大概數量在內。（本項於通知當事人時得不適用）
- DPO的姓名以及詳細連絡方式，或可以取得更多資訊的其他聯絡方式
- 描述關於個人資料受到侵害的結果，或有可能的結果
- 若無法同時提供資訊時，資訊應分階段提供，不得有進一步之無故遲延
- 為了因應個人資料受到侵害，描述控管者所採取的對應措施或預計要採取的對應措施。於必要時，包括為減輕因個人資料侵害所造成之不良影響之因應對策。

GDPR資料侵害通知之要件或義務（三）

■ 向當事人通知義務（Art.34）

- 控管者在個人資料受到侵害對於自然人之權利以及自由帶來高風險(a high risk to the rights and freedoms of natural persons)之情形，不得有不當的遲延，應立即通知（communicate）當事人關於個人資料遭到侵害的情形

■ 通知義務：無需立即通知當事人之情形（Art.34）

- 控管者已經採取合適技術性、組織性保護措施（appropriate technical and organisational protection measures），且此類措施已經被應用於例如加密技術等針對資料侵害影響之個人資料之中，尤其是那些未經授權任何人都無法得知的技術之情形
- 控管者已確實地採取相關措施，避免對自然人的權利以及自由受侵犯之高風險被實現之情形。

GDPR資料侵害通知之要件或義務（四）

- **通知義務：無需立即通知當事人之情形（Art.34）**
  - 需要不符比例努力（disproportionate effort）之情形，得以等同通知當事人的效果之手法進行通知，例如透過公開通知（public communications）或其他具有類似效果之措施。
- **記錄義務（Art.33(5)）**
  - 控管者應記載任何個人資料侵害，包括與個人資料侵害相關之事實、其影響及已採取之救濟措施。
- **GDPR資料侵害通知之效果**
  - 違反該通報義務時，有可能遭裁罰最高金額1,000萬歐元或前一會計年度全球年度銷售額之 2%兩者較高者之罰鍰
- **跨境處理發生個資侵害之處理**
  - 若有個資侵害需通報時，控管者須通報主要監管機關（Lead Supervisory Authority，LSA）（Art.55(1), 56(1)、(6)）

EDPB個人資料侵害通報之指引

■ 第2016/679號規則(GDPR)個人資料侵害通知之指引

- 個人資料侵害係指違反安全性導致傳輸、儲存或以其他方式運用之個人資料遭意外或非法破壞（destruction）、遺失、變更、未經授權揭露（unauthorised disclosure）或存取使用
- 個人資料侵害之類型
  - 機密性之侵害- 未經授權或意外揭露或存取個人資料
  - 完整性之侵害 - 未經授權或意外變更個人資料
  - 可用性之侵害 - 意外或未經授權遺失存取或破壞個人資料
- 知悉（aware）係指控管者就發生危及個人資料的安全事故已具有合理程度的確定時，例如遺失存有未加密個人資料隨身碟；意外取得未經授權揭露之客戶個人資料；罪犯駭入控管者之系統後並勒索贖金，在檢查其系統並確認已遭到攻擊後

EDPB個資外洩之通報案例指引（1/4）

■ 01/2021個資外洩之通知案例指引（Guidelines 01/2021 on Examples regarding Data Breach Notification）

- 個資外洩之通知案例指引，分為分為勒索軟體（Ransomware）攻擊、資料侵害攻擊、內部人為風險、硬體設備或紙本檔案遺失或偷竊、誤發郵件以及其他如社交工程等六大類
- 該指引將GDPR對控管者的要求分為三類
  - 無風險：記錄(document)任何個人資料侵害，包括與個人資料相關的事實違反、其影響和採取的補救措施（Art.35(5)）
  - 低風險：將個人資料侵害通知主管機構，除非資料侵害是對自然人的權利和自由不太可能造成風險（ unlikely to result in a risk ）
  - 高風險：當個人資料侵害發生，可能對自然人的權利和自由造成高風險時，將個人資料侵害通知當事人

EDPB個資外洩通報指引案例（2/4）

■ 銀行網站憑證填充攻擊（Credential stuffing）

- 銀行的網路銀行網站遭到攻擊。利用使用8個數字的固定簡單密碼（a fixed trivial password），對所有可能的用戶 ID進行登錄。因該銀行網站漏洞，在當事人的資訊（姓名、性別、出生日期和地點、財政代碼、用戶識別代碼）被洩露給攻擊者，即該使用密碼不正確或銀行賬戶不再使用。影響了大約 100.000 名客戶。駭客成功登錄大約 2.000 個使用簡單密碼的帳戶。
- 銀行可以夠識別所有非法登錄嘗試。根據反欺詐檢查並可以確認，在攻擊期間賬戶沒未任何交易。該銀行知道個資外洩是因為其安全運營中心檢測到大量針對該網站的登錄請求。
- 銀行通過關閉網站並強制客戶重置密碼來禁用登錄網站的可能性被盜用的賬戶。銀行僅將違規行為告知被洩露資料的帳戶，即密碼被洩露或資料被洩露的用戶揭露。

EDPB個資外洩通報指引案例（3/4）

■ 銀行網站憑證填充攻擊（Credential stuffing）

- 本案外洩的資料不僅是密碼與用戶名稱，且受影響人數不少。控管者（銀行）系統中的漏洞，根據 GDPR 第 24條第1項控管者之責任、第25條第1項隱私設計及預設，和第32條第1項資料安全義務，屬於必要的措施且需審視於必要時應予更新。被洩漏資料可用來標識特定當事人並包含其他資料（性別、日期和出生地），駭客得藉以猜測客戶的密碼或針對銀行客戶進行魚叉式網路釣魚（a spear phishing campaign ）
- 本次資料侵害，對所有相關當事人可能發生重大（如財務損失）和非物質損失（例如身份盜用或欺詐），被認為可能對權利和自由造成高風險。
- 本案控管者採取措施是充分的。修正網站的漏洞並採取適當措施來防止類似情形，例如網站使用雙因子身份驗證並升級強化客戶身份驗證

EDPB個資外洩通報指引案例（4/4）

■ 保險經紀人收到非屬其客戶之個人資料

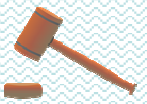
- 保險經紀人因收到電子郵件所附的 Excel 文件的錯誤設置，而得以近用非其所屬20幾位客戶資料。包括保險種類、金額但無其他敏感資料。保險經紀人需受職業保密義務約束，且是該電子郵件唯一收件人。
- 保險經紀人立刻向控管者通知個人資料洩露，控管者立即更正文件並再次發送，並要求保險經紀人刪除之前的 Excel 文件，並安排經紀人在書面聲明中確認刪除。
- 本案因涉及人數僅20餘人，資料洩漏並無敏感資料。屬於資料因意外傳輸受信任第三方。控管者採取教育訓練計畫，減少通過電子郵件交換文件，改使用專用系統來處理客戶資料，並在發送電子郵件前進行雙重檢查，被認定已經採取適當措施。本案僅需依GDPR第35條第5項進行記錄，無須通報主管機關與通知當事人

GDPR違反通報義務案例(1/2)

■ 2021年10月波蘭UODO 對Bank Millennium S.A. 因資料外洩而未通知主管機關與當事人，處以8萬歐元罰鍰

- 因Bank Millennium 兩位客戶於2019年向其Z. 分行申請開設帳戶，但申請文件包裹包含以下：申請人的姓名、姓氏、PESEL、註冊地址、銀行帳號、CIF 編號（銀行分配客戶編號）以及申請人的姓名等，在郵寄給總行時，被快遞公司 X Sp. 遺失。當事人未得到適當通知而向UODO投訴
- Bank Millennium認為該包裹未離開快遞公司 X Sp. ，且PESEL的遺失不會對當事人權利與自由構成高風險，所以未依GDPR第33條第1項通報UODO，同時該銀行依據ENISA 評估工具認定該事件僅構成中度風險未依GDPR第34條第1項通知當事人
- UODO認為丟失銀行客戶個人資料文件包裹，未經授權的接收者是否實際擁有並了解其他人的個資，仍存在風險的事實，存在侵犯當事人權利或自由的潛在風險，應將其視為高風險

GDPR違反通報義務案例(2/2)



■ 2021年10月波蘭UODO 對Bank Millennium S.A. 因資料外洩而未通知主管機關與當事人，處以8萬歐元罰鍰

- GDPR第33條第1項但書中只限於個人資料侵害無造成對當事人權利及自由之風險時，不需通報主管機關。同時向 UODO 通知資料外洩尤為重要，因 UODO可以驗證控制者的評估，該洩露是否會導致當事人的權利和自由的高風險
- UODO認為本案個人資料遺失對當事人權利和自由的風險應定義為高風險而非中度風險，因為個資遺失可能會導致導致身分盜用或偽造，或經濟損失。同時 PESEL 號碼是國家身分識別號碼，依GDPR 第 87 條應提供特別保護。雖然銀行表示兩年來並未發生勒索貸款之情事與企圖，且沒有收到當事人任何相關損失訊息。但UODO認為向當事人通知之義務，並非需要將違反的負面結果具體化，只要有構成此後果的可能性（風險）就足夠，認為Bank Millennium應依GDPR第34條第1項通知當事人

Urząd Ochrony Danych Osobowych

GDPR通知內容規範案例（1/2）

- **義大利資料保護機關（Garante）因網路電子郵件服務提供者Italiaonline Spa，對當事人進行個人資料侵害通知時，其內容違反GDPR第34條第2項，未提供特定且有效的資訊，Garante依第58條第2項令其限期改正**
  - 2019年6月7日Garante對webmail服務提供者Italiaonline Spa進行調查，發現通過WiFi熱點進行欺詐性訪問，影響約150萬webmail帳號的電子憑證安全。該業者雖然依GDPR第34條規定，以電子郵件通知當事人，要求重新設置密碼，同時依據已是否於48小時內重置密碼，分成兩種不同通知郵件。
  - 郵件內容以IT系統上的異常活動（unusual activities on our IT systems）來說明個資侵害事件，對於未修改密碼的客戶，建議加以修改，以避免未經授權訪問電子郵件帳戶的風險。

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

GDPR通知內容規範案例（2/2）

- **Garante要求Italiaonline Spa，進行個人資料侵害通知時，其內容應符合違反GDPR第34條第2項規定**
  - Garante認為該公司的通知內容應依GDPR第34條第2項規定，以清楚簡易之語言描述個人資料侵害，並至少應具備GDPR第33條第2項(b)、(c)、(d)各款規定資訊。包括告知DPO姓名及聯絡方式、描述個人資料侵害之可能結果、控管者已採取或預計採取處理個人資料侵害之措施，並參考Guidelines on Personal Data Breach Notification under Regulation 2016/679之規範
  - Garante命令該公司應提供資料侵害的類型及其可能的後果，並向用戶提供防止非法使用個人資料，尤其是身份盜用（identity thefts）的具體指導措施。重申告知受影響的用戶，例如若其使用這些密碼與被外洩的密碼相同或相似，則不要使用受影響憑證並更改密碼，以使用其他線上服務。

結語

結語

- 個資專責主管機關之殷切期待
- 個人資料外洩通知之修正方向
  - 立法體例：應將分散於不同主管機關個人資料檔案安全維護管理辦法之規範，在個資法予以適度整合。
  - 通報前提：「違反本法規定」之必要性？只要有個人資料侵害之事實？
  - 通報時間與方式：「查明」與「知悉」、72小時，得以電子方式，必要時可分次提供
  - 通報對象與順序:主管機關與當事人兩者都需要？應考量對當事人權利及自由之風險
  - 告知當事人之內容與格式規範
  - 後續之矯正措施與記錄義務

謝謝各位的聆聽