

歐盟發布《個資侵害通知範例指引》說明個資侵害案例解析以利個資事故因應



歐洲資料保護委員會（European Data Protection Board, EDPB）於2021年1月18日發布《個資侵害通知範例指引》（Guidelines 01/2021 on Examples regarding Data Breach Notification）草案，並進行為期六週之公眾諮詢。該指引針對2017年10月所發布之《個資侵害通知指引》（Guidelines on Personal data breach notification under Regulation 2016/679）透過案例分析進行補充說明，對於資料控制者如何識別侵害類別以及評估風險提出更詳細的實務建議，協助資料控制者處理資料外洩及風險評估考量因素之認定。

個資侵害係指違反安全性規定而導致傳輸、儲存或以其他方式處理之個資，遭意外或非法破壞、遺失、變更、未獲授權之揭露或近用之情形，由於個資事故將對資料主體可能造成重大不利影響，該指引首先要求資料控制者進行侵害類別之辨識，依據2017年指引將個資侵害分為機密性侵害（confidentiality breach）、完整性侵害（integrity breach）以及可用性侵害（availability breach）。而資料控制者最重要的義務在於主動識別系統漏洞，評估侵害對資料主體權利所產生之風險，制定適當計畫及程序採取適當因應措施，確定侵害事件之問題根因及安全漏洞，加強員工認知培訓及制定操作手冊，並確實記錄各項侵害行為，以提升個資事故因應效率及降低時間延誤。

此外，該指引彙整自GDPR實施以來個資侵害通知具體案例，分為勒索軟體攻擊、資料外洩攻擊、內部人為風險、硬體設備或紙本檔案失竊、誤發郵件以及電子郵件內容外洩，共六大主題十八件案例，針對不同程度風險提供最典型的正確及錯誤作法，並提出資料控制者有關預防潛在攻擊及減輕影響之措施建議。

相關連結

[歐盟資料保護工作小組修正通過個人資料侵害通報指引](#)

相關附件

[Guidelines 01/2021 on Examples regarding Data Breach Notification \(2021\) \[pdf\]](#)

你可能會想參加

- 製造業及技術服務業個資保護及資安落實－經濟部工業局112年企業個人資料保護暨資訊安全宣導說明會
- 【已額滿】2023科技研發法制推廣活動－科專個資及反詐騙實務講座
- 供應鏈資安國際法制與政策趨勢分享會
- 【實體】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
- 【線上】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
- 數位發展部數位產業署113年資訊服務業安維計畫常見問題分享說明會
- 商業服務業個資保護宣導說明會
- 個人資料保護新思維企業法遵論壇
- 【實體】2024科技研發法制推廣活動－科專個資及反詐騙實務講座
- 【直播】2024科技研發法制推廣活動－科專個資及反詐騙實務講座
- 中部場－商業服務業個資保護工作坊
- 南部場－商業服務業個資保護工作坊
- 北部場－商業服務業個資保護工作坊
- 數位發展部數位產業署113年資訊服務業者個資安維辦法宣導說明會



林佩瑩

組長 編譯整理

上稿時間：2021年04月

資料來源：

EUROPEAN DATA PROTECTION BOARD, Guidelines 01/2021 on Examples regarding Data Breach Notification (2021), available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf (last visited Apr. 1, 2021).

延伸閱讀：

李哲明，〈歐盟資料保護工作小組修正通過個人資料侵害通報指引〉，2018年5月，<https://stli.iii.org.tw/article-detail.aspx?tp=1&i=158&d=8028&no=64>（最後瀏覽日：2021/04/01）。

文章標籤

推薦文章