英國資訊委員辦公室（ICO）發布企業自行檢視是否符合歐盟一般資料保護規則之12步驟

英國作為歐洲金融重鎮，不論各行業均有蒐集、處理、利用歐盟會員國公民個人資料之可能，歐盟一般資料保護規則（General Data Protection Regulation，簡稱GDPR）作為歐盟資料保護之重要規則，英國企業初步應如何自我檢視組織內是否符合歐盟資料保護標準，英國資訊委員辦公室（Information Commissioner's Office, ICO）即扮演重要推手與協助角色。

英國ICO於2017年4月發布企業自行檢視是否符合GDPR之12步驟（Preparing for the General Data Protection Regulation（GDPR）-12 steps to take now），可供了解GDPR的輪廓與思考未來應如何因應：

1. 認知（Awareness）：認知GDPR帶來的改變，與未來將發生的問題與風險。
2. 盤點資料種類（Information you hold）：盤點目前持有個人資料，了解資料來源與傳輸流向，保留處理資料的紀錄。
3. 檢視外部隱私政策（Communicating privacy information）：重新檢視當前公告外部隱私政策，並及時對GDPR的施行擬定因應計畫。
4. 當事人權利（Individuals' rights）：檢視資料處理流程，確保已涵蓋GDPR賦予當事人如：告知權、接近權、更正權、刪除權、製給複本權、停止處理權、不受自動決策影響等相關權利。
5. 處理客戶取得資料請求（Subject access requests）：GDPR規定不能因為客戶提出取得資料請求而向其收費；限期於1個月內回覆客戶的請求；可對明顯無理或過度的請求加以拒絕或收費；如拒絕客戶請求則限期於1個月內須向其說明理由與救濟途徑等。
6. 處理個人資料須立於合法理由（Lawful basis for processing personal data）：可利用文書記錄與更新隱私聲明說明處理個人資料之合法理由。
7. 當事人同意（Consent）：重新檢視初時如何查找、紀錄與管理取得個人資料的同意，思考流程是否需要做出任何改變，如無法符合GDPR規定之標準，則須重新取得當事人同意。
8. 未成年人（Children）保護：思考是否需要制定年齡驗證措施；對於未成年人保護，考慮資料處理活動是否需取得其父母或監護人的同意。
9. 資料外洩（Data breaches）：有關資料外洩的偵測、報告與調查，確保已制定適當處理流程。
10. 資料保護設計與影響評估（Data Protection by Design and Data Protection Impact Assessments）：GDPR使資料保護設計與影響評估明文化。
11. 資料保護專責人員（Data Protection Officers）：須指定資料保護專責人員，並思考該專責人員於組織中的角色與定位。
12. 跨境傳輸（International）：如執行業務需跨越數個歐盟會員國境域，企業則須衡量資料監管機關為何。

相關連結

Guidance: what to expect and when, ICO.ORG.UK

相關附件

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now, ICO.ORG.UK [pdf]

你可能會想參加

→ 【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
→ 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
→ 電商零售業法制宣導說明會暨產學研座談會
→ 零售業個資保護宣導暨座談會
→ 零售業個資保護及資訊安全教育講習
→ 零售業個資保護及資訊安全教育講習

陳靜怡
法律研究員 編譯整理

上稿時間：2018年03月

資料來源：
1. Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now, ICO.ORG.UK, https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf（last visited Dec 23,2017）
2. Guidance: what to expect and when, ICO.ORG.UK, https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/guidance-what-to-expect-and-when/（last visited Dec 20,2017）

文章標籤

個資管理制度　個人資料保護與管理

推薦文章