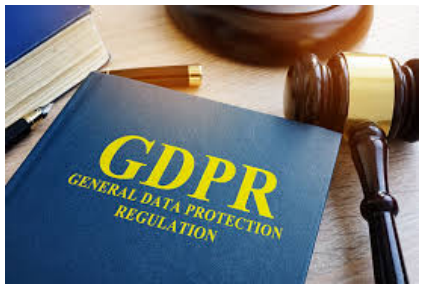
金融業因應歐盟一般資料保護規則(GDPR) 施行之相關作為

金融監督管理委員會



大 綱

一、我國金融業於歐盟地區設立情形及相關處置

二、我國金融業具體因應措施 - 以銀行業為例

三、金管會因應 GDPR 之具體協助措施

我國金融業於歐盟地區設立情形及相關處置

銀行業

- **6 家本國銀行：於歐盟境內設立 7 分行及 1 子行**
- 歐盟當地分行或子行處理歐盟自然人個資流程必須完整遵循 GDPR 及當地相關法規規定，而我國銀行總行就取得之歐盟自然人資料相關處理運用方式應遵循歐盟 GDPR 規定。
- 於歐盟當地設有據點之 6 家本國銀行，已採取適當措施。

我國金融業於歐盟地區設立情形及相關處置（續）

證券業

- **2 家證券公司：於歐盟境內設立 2 家子公司**
- 上開歐盟子公司之營運模式均係**轉介客戶至其他海外子公司開戶，且以法人戶為主**，原則不碰觸客戶個資，保有歐盟居民個資均為員工個資。

我國金融業於歐盟地區設立情形及相關處置

壽險業

- **2 家保險公司：於歐盟境內設立 8 家特殊目的公司（ SPV 公司）**
- 上開公司均**非從事保險業務**。該等公司除少數員工個資外，尚未涉及蒐集當地居民個資，經上開公司洽請顧問評估認為該等公司於歐盟地區設立之子公司不適用 GDPR 規定。

我國金融業具體因應措施 - 以銀行業為例

一、於歐盟當地有分支機構之銀行業

進行個資盤點

包括歐盟個資人數、業務範圍及是否適用 GDPR 之評估。

強化隱私資料之保護

1. 配合 GDPR 進行內部作業規範調整
2. 檢視網路資安防護系統
3. 建置個資外洩時之通報機制

GDPR 規範之比較

1. 完成法規差異分析
2. 評估建置個人資料可攜權、被遺忘權、限制權之機制。
3. 禁止犯罪前科資料之處理。

資料處理程序之調整

1. 檢視隱私資料蒐集、處理與利用的要件，包含：清楚、積極之同意、法定蒐集要件，配合調整相關契約條款。
2. 委託 / 諮詢外部顧問 / 律師提供專業協助處理，並依 GDPR 原則簽署同意遵循當地資料保護規範。

跨境傳輸之因應

因應 GDPR 跨境傳輸原則簽署 SCC (Standard Contractual Clauses) 或申請 BCRs(Binding Corporate Rules)

設置資料保護長

4 家已設置，1 家不設置，1 家不設置 DPO 但於倫敦設置聯絡窗口（DPR）。

我國金融業具體因應措施 - 以銀行業為例 (續)

二、於歐盟當地未有分支機構之銀行業

若其業務涉及對歐盟境內自然人提供商品或服務，或對歐盟境內自然人所為之監控，仍應適用 GDPR 規範

◆ 由總行或委託相關顧問公司協助進行差異性分析及影響範圍，並就個資蒐集、處理程序及個資當事人權利告知等事項，研議修正銀行個資同意書範本等相關規章。

◆取得歐盟自然人個資之銀行均已辦理法規差異分析，並已完成網路資安防護措施之檢視，及參加銀行公會及聯徵中心舉辦之相關宣導活動，並辦理內部教育訓練。

◆取得歐盟自然人個資較少之銀行，依據銀行公會推估，該等銀行被歐盟認為「有意圖為歐盟境內之自然人提供商品或服務」而適用歐盟 GDPR 之可能性甚低。

金管會因應 GDPR 之具體協助措施

於 GDPR 施行前，金管會已先請金融聯合徵信中心與銀行公會報告瞭解國內金融業者可能產生之影響、風險及後續之因應作法，並請該二單位於 107 年 5 月 17 日共同舉辦「金融業因應歐盟個人資料保護規則」研討會，藉此提供金融同業交流分享因應 GDPR 相關知識及經驗之機會。

督導銀行公會建置所屬會員公司適用歐盟 GDPR 規範資訊交流平臺，及透過洽詢歐盟當地顧問律師專業意見、彙整會員公司適用 GDPR 規範經驗分享、擬定個資保護檢視調整清單、指引及具體明確之因應措施方案，提供所屬會員遵循歐盟 GDPR 規範之參考。

督導證券期貨公會及保險公會協助所屬會員公司比照銀行公會之方式，以確保所屬業者落實 GDPR 之法令遵循。

金管會因應 GDPR 之具體協助措施 (續)

簡報結束