



# 銀行公會

The Bankers Association of the Republic of China

## 會訊 第一〇五期

中華民國 107 年 5 月

發行人 呂桔誠  
發行所 中華民國銀行公會  
地址 104 台北市德惠街 9 號 3 樓  
電話 (02)8596-2229  
傳真 (02)8596-2230  
創刊 中華民國 90 年 1 月  
設計美編 文匯印刷資訊處理有限公司

### 呂理事長出席 2018 年亞洲開發銀行第 51 屆理事會年會紀實

#### 歐興祥

銀行公會研究與發展委員會主任委員

## 壹、前言

### 一、亞洲開發銀行簡介

亞洲開發銀行（Asian Development Bank，簡稱亞銀或 ADB）成立於 1966 年 12 月，成立宗旨係致力於提高亞太地區人民的生活水準。成立初期有 31 個成員體，目前已經發展到 67 個成員體，其中 48 個來自亞太地區，19 個來自其它地區，我國是亞銀的創始會員國之一。有關亞銀成員體及股權比例詳如下表。

亞銀是亞洲最主要的區域性經濟發展金融機構，主要透過貸款、捐款、政策對話、技術援助和股權投資等援助方式，提供需要之協助；並透過區域論壇，線上諮詢，以及出版專項報告、系列刊物和書籍等多種形式，大力傳播開發資訊。亞銀理事會成員每年在年會中正式會晤一次，於每年 4 月底或 5 月初在其成員體國家召開理事會年會，今

（2018）年特地回到亞銀總部菲律賓馬尼拉舉行第 51 屆理事會年會，象徵區域金融合作邁入新的里程碑。

### 二、行程安排

我國代表團由財政部許部長虞哲率領，中央銀行、外交部、銀行公會、國際合作發展基金會等單位所組成，本會由呂理事長及研究與發展委員會主任委員歐興祥隨同代表團出席。為增進此行效益及提高與同業的交流與合作，呂理事長特別在 ADB 年會期間，與菲律賓中央銀行 (Bangko Sentral ng Pilipinas) 總裁 Mr. Nestor A. Espenilla, Jr. 會面，並與菲律賓中華銀行 (Rizal Commercial Banking Corporation, RCBC)、日本三井住友銀行 (Sumitomo Mitsui Banking Corporation, SMBC) 及瑞穗銀行 (Mizuho Bank Ltd.) 等亞洲重要金融業者進行雙邊會談，希冀開拓國內金融業者與當地金融業者業務往來及合作機會。



### 亞洲開發銀行成員體股權比例

截至2017年12月31日止

亞太地區成員體		股權比例（%）	非亞太地區成員體		股權比例（%）
1	阿富汗	0.034	1	奧地利	0.340
2	亞美尼亞	0.298	2	比利時	0.340
3	澳大利亞	5.786	3	加拿大	5.231
4	亞塞拜然	0.445	4	丹麥	0.340
5	孟加拉	1.021	5	芬蘭	0.340
6	不丹	0.006	6	法國	2.328
7	汶萊	0.352	7	德國	4.326
8	柬埔寨	0.049	8	愛爾蘭	0.340
9	中國大陸	6.444	9	義大利	1.807
10	庫克群島	0.003	10	盧森堡	0.340
11	斐濟	0.068	11	荷蘭	1.026
12	喬治亞	0.341	12	挪威	0.340
13	香港	0.545	13	葡萄牙	0.113
14	印度	6.331	14	西班牙	0.340
15	印尼	5.446	15	瑞典	0.340
16	日本	15.607	16	瑞士	0.584
17	哈薩克	0.806	17	土耳其	0.340
18	吉里巴斯	0.004	18	英國	2.042
19	南韓	5.038	19	美國	15.607
20	吉爾吉斯	0.299	小計		36.467
21	寮國	0.014			
22	馬來西亞	2.723			
23	馬爾地夫	0.004			
24	馬紹爾群島	0.003			
25	密克羅尼西亞	0.004			
26	蒙古	0.015			
27	緬甸	0.545			
28	諾魯	0.004			
29	尼泊爾	0.147			
30	紐西蘭	1.536			
31	巴基斯坦	2.178			
32	帛琉	0.003			
33	巴布亞紐幾內亞	0.094			
34	菲律賓	2.383			
35	薩摩亞	0.003			
36	新加坡	0.340			
37	索羅門群島	0.007			
38	斯里蘭卡	0.580			
39	臺灣	1.089			
40	塔吉克	0.286			
41	泰國	1.362			
42	東帝汶	0.010			
43	東加	0.004			
44	土庫曼	0.253			
45	吐瓦魯	0.001			
46	烏茲別克	0.674			
47	萬那杜	0.007			
48	越南	0.341			
小計		63.533	總計		100.00

註：截至2017年12月31日止，亞洲開發銀行成員體共67個，其中48個來自亞太地區，19個來自其它地區。

資料來源：亞洲開發銀行2017年年報

## 貳、第 51 屆 ADB 年會主要會議或活動內容

### 一、年會主題

第 51 屆 ADB 年會於 5 月 3 日至 6 日假馬尼拉舉行，年會主題為「Linking People and Economies for Inclusive Growth (連接人民與經濟，共同推動包容性成長)」。年會期間之會議重點關注全球化、亞洲工作機會、金融科技、氣候變遷、增加婦女在企業的機會、提升年長者的科技使用、運用有效方式促成包容性成長等議題。本屆年會，計有來自各國財政部、中央銀行、政府官員、學者、民營企業、國際組織等約 4,000 多名代表參與。

### 二、開幕典禮

ADB 理事年會開幕典禮於 5 月 5 日上午 10 時 30 分舉行，亞銀總裁中尾武彥在開幕典禮中致詞。中尾總裁表示，隨全球及區域貿易成長漸趨穩健，2017 年開發中亞洲國家的經濟成長率為 6.1%，今年亦將成長 6.0%，他對亞洲經濟成長持樂觀看法。其次，他強調為了實現「一個繁榮的、具包容性的、韌性及可持續性的亞太地區 (a prosperous, inclusive, resilient, and sustainable Asia and the Pacific)」之願景，ADB 推出新的長期戰略「2030 發展策略 (Strategy 2030)」，包含：(1) 解決亞太地區持續存在的貧困和不平等問題；(2) 加速兩性平等進程；(3) 加大應對氣候變遷力度，並加強環境可持續性；(4) 建設具競爭力、環保、韌性及包容性的宜居城市；(5) 推動農村發展和糧食安全；(6) 加強治理；(7) 促進區域合作和一體化；(8) 動員私部門資源來滿足區域發展的巨大融資需求；(9) 進一步加強 ADB 作為知識提供者和促進者的角色；(10) 追求更強、更好、更快的 ADB 等十大重點。

### 三、理事會議

ADB 年會的另一項重要會議為於 5 月 5 日 13:00-17:00 舉行的理事會議，由各理事會員之代表進行報告。我國代表財政部許部長虞哲報告中除對亞銀新策略表達深切肯定與期許，並介紹臺灣提高勞動生產力的具體作法，如稅制改革、制定專法、修正公布「產業創新條例」部分條文、制定「金融科技發展與創新實驗條例」等；此外，許部長也就



呂理事長與日本央行總裁黑田東彥 (Mr. Haruhiko Kuroda) 於 ADB 年會期間合影

臺灣如何扶植金融創新產業、維護性別平權、協助女性創業、推動新南向政策，以及增進臺灣與亞銀會員國合作等，逐一加以說明。

### 四、其他重要活動

除了 ADB 年會期間相關會議及研討會外，亞銀總裁、主辦國分別於 5 月 4 日及 5 日舉辦晚宴，宴請來自各國與會代表，並進行交流聯誼。呂理事長在 5 月 4 日亞銀總裁晚會中，分別與亞銀總裁中尾武彥及日本央行總裁黑田東彥寒暄致意，並合影留念。

### 參、與亞洲金融業雙邊會談

本會呂理事長於出席第 51 屆 ADB 年會期間，特別拜會菲律賓中央銀行總裁 Mr. Nestor A. Espenilla, Jr.，藉以爭取臺灣銀行業者進入當地市場之契機及放寬業務限制，進而滿足台商赴菲國投資的各項金融需求。呂理事長首先感謝菲律賓中央銀行同意臺灣銀行馬尼拉代表人辦事處設立，該辦事處預計於今 (2018) 年第 3 季開業，未來將有助於臺菲雙方金融往來。雙方皆各自樂觀看待臺菲經濟金融發展，並認為未來應強化交流，營造有利雙方合





呂理事長與亞銀總裁中尾武彥 (Mr. Takehiko Nakao) 於 ADB 年會期間合影



呂理事長與菲律賓央行總裁 Mr. Nestor A. Espenilla, Jr. 伉儷合影

作往來之經濟金融環境，創造共利雙贏局面。

為了增進與亞洲金融業的合作關係，呂理事長在本屆 ADB 年會期間，積極與菲律賓的中華銀行、日本的三井住友銀行、瑞穗銀行等多家亞洲指標性銀行的負責人進行雙邊洽談與交流，就未來兩國金融業者合作方向獲致高度共識，成果豐碩。

## 肆、結語

ADB 為重要之國際組織，對亞洲各國的經濟發展及基礎建設扮演著相當重要的角色。臺灣為 ADB 創始會員國，多年來善盡會員國的權利與義務，截

至目前為止，臺灣對亞洲開發基金的捐款累計已達 1.1 億美元，對於協助區域內貧窮國家改善生活水準貢獻良多。

銀行公會為充分發揮協助會員銀行之功能與角色，藉由參加 ADB 年會，不僅代表臺灣銀行業與各國金融同業建立了良好的交流平台，開拓與亞洲各國金融同業合作機會，亦可汲取國際知名金融業優勢經驗。此外，新南向政策為政府現階段最為重要的政策之一，透過出席 ADB 年會增進我國與東協及南亞地區之連結，更為布局新南向市場締造加乘效果。

## 中華民國銀行公會二度舉辦紐約「海外分區經理人、法遵人員暨內稽內控人員研討會」活動紀要

### 溫國恩

銀行公會業務組組長

## 壹、緣由

中華民國銀行公會（下稱銀行公會）為強化金融法令遵循並維護金融秩序，避免國銀發生未遵守法令或不合規等違失事件，繼去（106）年 1 月、4 月、7 月協同台灣金融研訓院赴紐約、香港、倫敦舉辦「海外分區經理人、法遵人員暨內稽內控研討

會」後，今（107）年 3 月 29 日至 30 日第二度於美國紐約舉辦本研討會活動，在美設有據點的本國銀行均熱烈參與，共計有 8 家本國銀行董事長、總經理親率總行高層法令遵循、內部稽核或負責國際業務之主管出席，充分展現由上而下重視法遵之文化，各銀行總行及海外分 / 子行約 120 位參與，期間交流熱烈，成果豐碩。



中華民國銀行公會 107 年 3 月 29 日至 30 日於紐約二度舉辦「海外分區經理人、法遵人員暨內稽內控研討會」，呂理事長桔誠與金管會銀行局莊副局長琇媛、金管會紐約辦事處黃主任錫和及與會銀行董事長合影

## 貳、研討會議程內容

本次研討會為期一天半，於銀行公會呂理事長致詞中揭開序幕，銀行公會呂理事長表示，今年是銀行公會第二度在紐約舉辦研討會，顯示臺灣銀行業對美國市場之重視與珍惜。臺灣銀行業雖面臨外在經營環境日趨複雜，偶有防制洗錢違失與資安控管弱點事件發生，經營挑戰性增高，但危機就是轉機，近期臺灣銀行業均致力加強總行對國外分／子行之管理，並逐年增加海外分行法遵人員之專業要求及配置比重，在積極布局海外增設據點的同時，亦加強建立更完善的法令遵循、內控內稽制度，期落實遵法的企業文化。

本次研討會除邀請金管會銀行局莊副局長琇媛，亦邀請著名外資法律機構及當地金融業法遵高層主管進行專題演講及參與綜合座談，包括：(1) 紐約梅隆銀行（BNY Mellon）執行副總經理 Ms. Sandra L. Depoalo；(2) 安理國際律師事務所（Allen

& Overy LLP）資深顧問 Ms. Jillian Ashley；(3) Hogan Lovells 法律事務所資深副總裁 Ms. Stephanie Gosnell Handler；(4) 普華商務法律事務所（PwC）金融犯罪部門負責人 Mr. Daniel Tannebaum；(5) Bonita Jones & Associates LLC 總裁 Ms. Bonita G. Jones 等法遵專家。其中，曾經在美國聯邦準備銀行（Federal Reserve Bank）任職 30 年資深檢查員，亦為經常接受美國銀行公會、紐約銀行公會邀請擔任講座之著名講師的 Bonita Jones，本次研討會除參加綜合座談外，並擔任本次研討會壓軸講座，與學員交流互動熱烈。

本次研討會中，各與會法遵專家除了就法令遵循（尤其是防制洗錢與打擊資恐、銀行保密法案等）、資訊安全、實質受益人查核、監理與檢查制度、內部控制與稽核程序、風險管理策略等重點議題，分享其專業見解外，亦針對美國近期發布之重要法規（例如：NYDFS Part500 and Part504）及實務執行重點進行深入剖析及座談交流，期增進台灣銀



行業者對美國金融法規之了解、促進台美雙方金融交流，藉以強化國銀法遵意識及健全法遵制度發展。

金管會銀行局莊副局長琇媛於專題演講時也特別期許，近期金管會陸續發布修正金融業相關內部控制及稽核制度實施辦法，針對銀行業的部分，首重強化法遵與風險控管機制、加強公司治理及建置資安專責制度等，具體作為係推動建立大型銀行差異化管理機制，並要求全體金融控股公司及銀行業應建立內部檢舉制度，希望金融控股公司及銀行業應依法落實，以創造安全之金融內控環境。

## 參、結語

研討會活動尾聲，呂理事長也特別感謝金管會、金管會紐約辦事處及專家、講師們的參與及分享。本次研討會多位銀行董事長、總經理親赴紐約與會，也創下銀行公會歷年來海外研討會參加層級最高的

紀錄。會中主管機關、國內外分行與會代表均踴躍發言提問，外資講座與我國金融同業間亦進行雙向深度交流及溝通，彼此分享寶貴的法遵理論與實務工作經驗，可說是一次相當難得的法遵國際交流盛會。

呂理事長強調，這次第二度於美國紐約舉辦本研討會，就是要向美方監理單位展現台資銀行戮力提昇法令遵循的決心，並已獲得美方正面評價，期許我國銀行業都能翻轉思維，使法令遵循、資訊安全成為銀行從業人員的 DNA，以提升臺灣銀行業之國際聲譽。

為延續我國金融業與國外監理單位間的互信及友好關係，未來銀行公會仍將與主管機關及會員銀行共同攜手合作，每年選擇適當的時間及地區舉辦海外法遵研討會，以持續展現國銀重視法遵之企業文化及強化落實法令遵循之決心。

# 歐盟個人資料保護規則（GDPR）簡介 ——兼論對我國銀行業的影響與因應

葉建廷

建業法律事務所主持律師

## 壹、前言

歐洲議會（European Parliament）及歐盟理事會（Council of the European Union）於 2016 年 5 月 24 日通過歐盟規則第 2016/679 號「個人資料保護規則」（General Data Protection Regulation，下稱「GDPR」），並訂有二年的過渡期間，將於 2018 年 5 月 25 日開始全面適用於歐洲經濟區（European Economic Area）（註 1），以取代 1995 年所制定之歐盟指令第 95/46/EC 號「個人資料保護指令」（Data Protection Directive）。有鑑於 GDPR 並非僅適用於在歐盟境內蒐集、處理及利用個人資料（註 2），甚至控管者（註 3）或處理者（註 4）在歐盟境內並無設立分支機構亦有可能須適用歐盟 GDPR，因此我國銀行業不論在歐盟是否設立分支機構（establishment），均不得輕忽歐盟 GDPR 施行後

可能帶來之法律遵循風險。本文將簡介歐盟 GDPR 之規範重點以及探討歐盟 GDPR 適用後我國銀行業可能面臨之法律遵循問題及因應措施。

## 貳、歐盟個人資料保護規則（GDPR）概述

歐盟 GDPR 主要係為保護自然人個人資料之蒐集、處理及利用（以下統稱處理）及個人資料之自由流通。歐盟 GDPR 將取代原有之歐盟指令第 95/46/EC 號個人資料保護指令（註 5），就歐盟法性質而言，歐盟指令（Directive）為歐盟所訂定之最低標準，各會員國需要自行訂定國內法以施行歐盟指令，而因為指令僅是最低標準，因此各會員國可自行訂定較嚴格之規範，致使各會員國目前就個人資料保護之法令規定有所不同。而本次歐盟 GDPR 係以規則（Regulation）之位階立法，規則於各會員



國間將自動生效及適用，無需由各會員國將其轉化為國內法，而使歐盟境內個人資料保護規定一致化，但歐盟 GDPR 中將某些內容交由各會員國自行決定如何規範（註 6），各會員國亦可自行決定是否要修訂國內個人資料保護法令，將歐盟 GDPR 之相關規定納入，或使國內法規定與歐盟 GDPR 規定相符且無牴觸，或是針對歐盟 GDPR 未規範的部分進行補充規範。而歐盟 GDPR 之監管及執行將會由各會員國之相關監管機關為之。謹將歐盟 GDPR 之重要條文簡介如下：

## 一、個人資料定義及特殊類型之個人資料處理

歐盟 GDPR 擴大了對個人資料之定義，依歐盟 GDPR 第 4 條第 (1) 項規定（註 7），「個人資料」係包含有關識別或可得識別的自然人（「資料主體」）之任何資料；可得識別自然人係指得以直接或間接識別該自然人，特別是參考諸如姓名、身分證統一編號、位置資料、網路識別碼或一個或多個該自然人之身體、生理、基因、心理、經濟、文化或社會認同等具體因素之識別工具。依據此定義，諸如位址資料（如 GPS 定位）、網路識別碼（如 IP 位置、Cookies）、或一個或多個自然人之身體、生理、基因、心理、經濟、文化或社會認同等具體因素等資料均屬歐盟 GDPR 定義之個人資料。

此外，歐盟 GDPR 第 9 條規定，原則上禁止處理特殊類型之個人資料，除非在某些特定前提下，例如取得當事人明確同意才可處理。而特殊類型之個人資料涵蓋揭露種族或人種、政治意見、宗教或哲學信仰或工會會員之個人資料、基因資料、用以識別自然人之生物特徵識別資料、與健康相關或與自然人之性生活或性傾向有關之個人資料。同時，歐盟 GDPR 第 10 條亦明確禁止涉及前科及犯罪之個人資料處理，該等資料僅能於公務機關控管下進行處理或保管，留存任何全面性的前科紀錄僅限由公務機關控管保存。

## 二、實體適用範圍（Material scope）及領土適用範圍（Territorial scope）

依歐盟 GDPR 第 2 條規定，此規則適用於所有以自動化方式處理之個人資料，及其他非自動化方式處理而構成檔案系統之一部分的個人資料。而依

歐盟 GDPR 第 3 條規定，其領土適用範圍如下：

1. 歐盟 GDPR 適用於控管者或處理者在歐盟境內之分支機構所為之個人資料處理活動，且不問該處理是否發生於歐盟境內。
2. 歐盟 GDPR 適用於非設立於歐盟境內之控管者或處理者，對於歐盟境內之資料主體（data subjects，即當事人）所為涉及下列事項之一的個人資料處理：
  - (1) 對歐盟境內之資料主體提供商品或服務，不問是否需要資料主體付款。
  - (2) 對於資料主體於歐盟內所為行為監控。
3. 歐盟 GDPR 適用於非設立於歐盟境內之控管者，但在會員國法律依國際公法可得適用領域內所為之個人資料處理。

綜觀上述規定，歐盟 GDPR 除採取屬地主義外，亦有域外效力，在特定條件下適用於非設立於歐盟境內之控管者或處理者其所持有或控管之歐盟資料主體（當事人）之個人資料。

## 三、個人資料處理原則及處理之合法性（Lawfulness of processing）

依歐盟 GDPR 第 5 條規定，個人資料之處理應遵守以下原則：

1. 合法性、公正性及透明度（lawfulness, fairness and transparency）；
2. 目的限制（purpose limitation），即蒐集目的須特定、明確及合法，且不得為該等目的以外之進階處理；
3. 資料蒐集最少原則（data minimization），為與處理目的適當及相關，並限於處理目的所必要；
4. 正確性（accuracy），必要時應隨時更新個人資料，考慮個人資料處理之目的，應採取一切合理措施，確保不正確之個人資料立即被刪除或更正；
5. 儲存限制（storage limitation），即儲存期間不長於處理目的所必要之期間；
6. 完整性和保密性（integrity and confidentiality），即處理應以確保個人資料適當安全性之方式為之，包括使用適當之技術上或組織上之措施，以防止未經授權或非法處理，並防止意外遺失、破壞或損壞。而上述原則控管者應



有責任 (accountability) 遵守並能證明其有遵守。

而歐盟 GDPR 第 6 條第 1 項規定，對於個人資料之合法處理，應至少符合下列要件之一：

1. 資料主體同意 (註 8) 為一個或多個特定目的處理其個人資料；
2. 處理係為向身為契約當事人之資料主體履行契約所必須者，或在締約前，應資料主體之要求，所必須採取之步驟；
3. 處理係控管者為遵守法律義務所必須者；
4. 處理係為保護資料主體或他人重大利益所必須者；
5. 處理係為符合公共利益執行職務或委託控管者行使公權力所必須者；
6. 處理係控管者或第三者為追求正當利益之目的所必須者，但該個人資料保護之資料主體之利益或基本權與自由優先於該等利益，特別是該資料主體為兒童時，不適用之。

#### 四、資料主體之權利 (Rights of the data subject)

##### (一) 透明度及管道 (Transparency and modalities)

1. 透明資訊、溝通及接近管道 (歐盟 GDPR 第 12 條第 1 項)：採取適當措施，以簡明、透明、易懂且方便取得之格式，並採用清楚簡易之語言，提供關於對資料主體 (當事人) 所為處理之任何溝通。
2. 資料主體行使權利 (歐盟 GDPR 第 12 條第 2 項)：控管者有義務促使資料主體依歐盟 GDPR 第 15 條至第 22 條之規定行使其權利，且不得拒絕，除非控管者證明其無從識別該資料主體之地位。
3. 處理時限 (歐盟 GDPR 第 12 條第 3 至 4 項)：控管者最遲應於收到資料主體請求後一個月內提供相關資訊，必要時得再延長兩個月，控管者應於收到請求後一個月內通知資料主體該展期，並說明遲延之原因。如控管者不會依資料主體之要求採取行動，應立即且最遲於收到資料主體要求之一個月內附具理由告知該資料主體，並敘明向監管機關提出申訴及尋求司法救濟之可能性。
4. 無償提供 (歐盟 GDPR 第 12 條第 5 項)：

就資料主體依歐盟 GDPR 第 15 條至第 22 條及第 34 條規定要求控管者提供之資訊或請求行使之權利所採取之任何行動，應無償提供之，如當事人之請求明顯無理由或過度者，尤其是基於該等請求過於重複者，控管者得考量所要求提供之資訊或溝通或採取行動之行政成本，收取適當費用，或拒絕該請求，而控管者應就該請求之明顯無理由或過度性負舉證責任。

##### (二) 接近使用權 (Right of access) (歐盟 GDPR 第 15 條)：

資料主體有權向控管者確認其個人資料是否正被處理，並取得相關處理資訊。例如處理之目的、個人資料所涉及之類型、個人資料揭露或接收對象、個人資料將被儲存之預期期間、非從當事人直接蒐集所得之個人資料之來源、若有自動決策 (automated decision) 或建檔 (profiling)，處理個人資料所涉及之邏輯性、重要性及預設結果，以及若個人資料若被傳輸至第三國，當事人有權獲知相關傳輸之保護措施及取得正在處理之個人資料影本等。

##### (三) 更正權 (Right to rectification) (歐盟 GDPR 第 16 條)：

資料主體應有權使控管者更正其不正確之個人資料，不得無故拖延。考量到處理之目的，資料主體應有權完整化其有欠缺之個人資料，包括以提供補充說明之方式。

##### (四) 刪除權 (被遺忘權) (Right to erasure “Right to be forgotten”) (歐盟 GDPR 第 17 條)：

在特定情形下 (如資料主體撤回其同意)，資料主體應有權使控管者刪除其個人資料，且控管者應有義務刪除該個人資料，不得無故拖延。

##### (五) 資料可攜權 (Right to data portability) (歐盟 GDPR 第 20 條)：

資料主體有權以有結構的、通常使用的、機器可讀的形式取得其提供予控管者之個人資料，且有權將該個人資料傳輸給其他控管者。如技術許可時，資料主體亦有權使該個人資料由一控管者直接傳輸予其他控管者。

##### (六) 個人化之自動決策，包括建檔 (Automated individual decision-making, including profiling)

(歐盟 GDPR 第 22 條)：除特定情形外，資



料主體有權不受僅基於自動化處理（包括建構）所做成而對其產生法律效果或類似之重大影響之決策所拘束。

## 五、歐盟境內代表（Representatives）

依歐盟 GDPR 第 27 條規定，若非設立於歐盟境內之控管者或處理者，有處理位於歐盟資料主體之個人資料，且該個人資料處理有歐盟 GDPR 第 3 條第 2 項規定適用（即對歐盟境內之資料主體提供商品或服務，不問是否需要當事人付款，或對於當事人於歐盟內所為行為進行監控時），控管者或處理者應以書面指定歐盟境內之代表，除非該個人資料處理係出於偶然（occasional），不包括大規模涉及特殊類型之個人資料處理、或涉及前科及犯罪之個人資料的處理，且考量處理之本質、過程、範圍與目的，其不會對當事人之權利與自由造成風險。境內代表應設立於資料主體所在之一個會員國境內，且可被控管者或處理者授權獨自代表，或偕同控管者或處理者針對歐盟 GDPR 之遵循面對監管機關或資料主體，惟控管者或處理者所指定之代表不得影響得對於控管者或處理者本身提起之法律行動。

## 六、個人資料侵害的通報

歐盟 GDPR 第 34 條規定，於個人資料侵害發生時，且該侵害可能導致資料主體權利及自由之高風險時，控管者應通知資料主體，不得無故遲延，但若控管者針對個人資料侵害已執行適當之科技化與有組織之保護措施、已使未獲授權接近使用之人無法識別個人資料者（如加密）、控管者已採取後續措施，確保對當事人權利及自由之高風險已不會實現、或個別通知不符比例原則時（於此情形，應有公共溝通或類似措施取代之，使資料主體獲相同有效之通知），應無須被要求通知資料主體。除向資料主體通報外，歐盟 GDPR 第 33 條規定，控管者應於發現個人資料侵害後 72 小時內向監管機關通報，但個人資料侵害無造成對當事人權利及自由之風險時，不在此限。

## 七、資料保護長（Data protection officer）

依歐盟 GDPR 第 37 條規定，當個人資料控管者及處理者之核心活動，包括依其本質、範圍及/或其目的，需要定期且系統性地大規模監控當事

人，或控管者或處理者之核心活動包括大規模處理特殊類型之資料及前科與犯罪相關之個人資料時，控管者及處理者須指定資料保護長（data protection officer）。企業集團得指定同一名資料保護長，只要該資料保護長對各分支機構是易於接近的。

資料保護長應依專業資格，尤其資料保護法律與實踐之專業知識及完成歐盟 GDPR 第 39 條所稱職務之能力。資料保護長得為控管者或處理者之員工或委任之外部顧問，且歐盟 GDPR 第 38 條規定，資料保護長應具獨立性，控管者或處理者針對資料保護長職務之執行不得給予任何指示，資料保護長應直接向處理者或控管者之最高管理階層報告，且其不得因執行職務而被控管者或處理者解任或處罰。

## 八、國際傳輸

依歐盟 GDPR 第 45、46 及 49 條規定，僅有符合下列情形之一者，方能將個人資料移轉至第三國或國際組織：

1. 具備充足程度保護之決定（adequacy decision）：歐盟 GDPR 第 45 條第 1 項規定，歐盟執委會決定所傳送之第三國或國際組織具備充足程度之保護，經歐盟執委會評估保護之充足程度後認可之國家，歐盟執委會應提供定期檢驗保護程度是否充足之機制。
2. 適當保護措施之提供：歐盟 GDPR 第 46 條規定，雖欠缺執委會具備充足程度保護之決定，但資料控管者或處理者得提供適當保護措施，且資料主體之權利得為執行，並具備有效權利救濟時，亦得進行國際傳輸。適當保護措施包括經監管機關核准具有拘束力的企業守則（Binding corporate rules）、監管機關採行，並由執委會依歐盟 GDPR 第 93 條第 2 項之檢驗程序核准之標準資料保護條款（Standard contractual clauses）；或經監管機關核准之控管者與接收者之契約條款。
3. 若無具備充足程度保護之決定或提供適當保護措施時，在符合歐盟 GDPR 第 49 條規定之特定情形下，國際傳輸亦被允許。例如，經通知欠缺充足程度保護決定及適當保護措施、該資料傳輸可能之風險，當事人明確同意國際傳輸，或國際傳輸對履行當事人與控



管者間契約，或依當事人之請求執行契約前之措施為必要。

## 九、裁罰

若個人資料控管者及處理者違反歐盟 GDPR 規定，除民、刑事責任外，亦需負擔行政責任。依歐盟 GDPR 第 83 條規定，違反程序規定等情節輕微者，最高可裁處至 1,000 萬歐元，或如為企業者，最高達前一會計年度全球年營業額的 2%，並以較高者為準；就實質侵害個人資料之情形者，最高可達 2,000 萬歐元，如為企業者，最高達前一會計年度全球營業額的 4%，並以較高者為準。而刑事責任部分，依歐盟 GDPR 第 84 條規定，由歐盟各會員國自行制定違反歐盟 GDPR 所適用其他罰則之規定。

## 參、我國銀行業適用歐盟 GDPR 可能面臨之問題及因應措施

針對歐盟 GDPR 之施行，對我國銀行業之影響，可區分為在歐盟當地設有分支機構（分行或子行）之銀行，及在歐盟當地無分支機構之銀行。就前者而言，因在歐盟當地設有分行或子行，依歐盟 GDPR 第 3 條第 1 項規定，為歐盟 GDPR 之適用範圍，自應遵循歐盟 GDPR 規定蒐集、處理及利用，歐盟境內資料主體個人資料流程均須完整遵循歐盟 GDPR 及當地相關會員國之法規，包含取得客戶資訊、當地員工聘僱資料等；至於未於歐盟當地設有分行或子行等分支機構之銀行，依歐盟 GDPR 第 3 條第 2 項規定，如有對歐盟境內之資料主體提供商品或服務，不問是否需要資料主體付款，抑或對於資料主體於歐盟內所為行為監控時，亦應適用歐盟 GDPR。果爾，自應依歐盟 GDPR 規定處理歐盟境內資料主體的個人資料、進行國際傳輸、於歐盟境內設立代表或設置資料保護長。

再者，如前所述，歐盟 GDPR 對我國銀行業確有影響，惟有鑑於歐盟 GDPR 之規定及我國個人資料保護法之規範內容仍有差異，建議我國銀行業應就下述各面向採取相關的因應措施：

### 一、適用範圍

我國個人資料保護法僅概括式兼採屬地主義與域外效力（註 9），至於何謂領域外對我國國民

個人資料蒐集、處理或利用並未有明確定義。歐盟 GDPR 亦兼採屬地主義與域外效力，但依歐盟 GDPR 第 3 條第 2 項規定，對於非設立於歐盟境內之控管者或處理者對於歐盟境內之資料主體所為之個人資料處理情形在何種情形下應有歐盟 GDPR 之適用，則有明確之定義。因此我國銀行業應自行盤點是否有歐盟 GDPR 第 3 條所述之情事之一，做為檢視是否有歐盟 GDPR 適用之第一步驟。

## 二、個資之定義（含特種個資）

歐盟 GDPR 對於個人資料之定義較我國個人資料保護法廣泛，包含有關識別或可得識別的自然人之任何資料。列舉項目包含位址資料（如 GPS 定位）、網路識別碼（IP 位置、Cookies）、或一個或多個自然人之身體、生理、基因、心理、經濟、文化或社會認同等具體因素。針對特種個資歐盟 GDPR 亦有不同定義，就犯罪前科之部分，我國個人資料保護法第 6 條第 1 項第 6 款允許經當事人書面同意得蒐集、處理或利用，但依據歐盟 GDPR 第 10 條規定，犯罪前科僅能在公務機關控制下進行蒐集、處理。因此，針對個資定義之擴大，建議我國銀行應盤點目前所蒐集歐盟境內資料主體及當地聘僱員工之相關資料，是否有符合歐盟 GDPR 第 4 條第 1 項及第 9 條所定義之個人資料，並應限制特種個資「犯罪前科」的蒐集、處理及利用。

## 三、國際傳輸

我國個人資料保護法原則許可國際傳輸，僅例外予以限制（註 10），依歐盟 GDPR 第 45、46 及 49 條規定則原則禁止國際傳輸，僅於符合前述所揭示三種情形之一，始得進行國際傳輸。

就此，我國銀行若欲將個人資料自歐盟境內傳輸至歐盟境外時，須比照歐盟 GDPR 的前揭規定辦理，因我國目前並非歐盟執委會所認可有充足程度保護之國家，因此我國銀行進行國際傳輸須遵守適當保護措施。例如制訂經主管機關核准之具拘束力的企業守則，監管機關採行，並由執委會依歐盟 GDPR 第 93 條第 2 項之檢驗程序核准之標準資料保護條款，或經監管機關核准之控管者與接收者之契約條款，若無上述適當保護措施之一時，則須依歐

盟 GDPR 第 49 條規定進行國際傳輸。例如：經當事人明確同意移轉、履行資料主體與控管者間契約所為必要之移轉或依資料主體之請求執行契約前之措施為必要。

#### 四、個人資料侵害通報

我國個人資料保護法僅就個人資料外洩時要求通知當事人（註 11），歐盟 GDPR 第 33 條則進一步要求向監管機關通報。因此，若有個人資料侵害之情形時，建議我國銀行應比照歐盟 GDPR 的規定辦理，除通知資料主體外，亦需於發現個人資料侵害後 72 小時內向當地國的監管機關通報。

#### 五、非設立於歐盟境內控管者或處理者之代表

我國個人資料保護法並無指定控管者或處理者代表之要求，而歐盟 GDPR 第 27 條則規定非設立於歐盟境內控管者或處理者應指定歐盟境內之代表，除非資料處理係出於偶然、不包括大規模涉及特殊類型之個人資料處理、或涉及前科及犯罪之個人資料的處理，且考量處理之本質、過程、範圍與目的，其不會對當事人之權利與自由造成風險。是以，我國銀行雖未在歐盟設立分支機構，但仍應就此予以評估是否符合歐盟 GDPR 規定應設立歐盟境內代表之條件，並依相關規定辦理。

#### 六、資料保護長之設置

我國個人資料保護法第 18 條僅規定公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。惟歐盟 GDPR 第 37 條規定，要求符合特定情形時，控管者或處理者應設置資料保護長。與金融機構相關之部分，在有大規模且系統性定期監控資料主體或大規模處理特殊個資之情形時即須設置，而控管者或處理者可以委外聘雇專業團隊擔任資料保護長，並非一定須於內部設置專任之資料保護長。建議我國銀行應依歐盟 GDPR 前揭規定，評估是否有設置資料保護長之必要，且企業集團得指定同一名資料保護長，因此銀行分行或子行與總行得指定同一人擔任之。

#### 肆、結語

為保障人格權基本人權，各國對於個人資料的保護，均不遺餘力。我國銀行業除應遵守個人資料保護法之外，如符合適用歐盟 GDPR 之情形，亦應同時遵守前揭規定，二者之規範雖有所差異，惟其立法目的均為促進個人資料之合理利用。有鑑於歐盟 GDPR 將於 2018 年 5 月 25 日起全面適用，我國銀行業應確實評估是否有歐盟 GDPR 的適用，及早擬定因應策略及具體措施，以確保於辦理各項業務時，同時恪遵相關法令規定。

註 1：歐洲經濟區係由歐盟 28 個會員國及四個歐洲自由貿易聯盟成員中的三國：冰島、列支敦士登和挪威（瑞士除外）所組成。

註 2：歐盟 GDPR 前言第 (14) 點規定：「本規則所保護者，係不論當事人之國籍或住居所，凡涉及其個人資料之處理均屬之。本規則並未涵蓋法人及具法人資格之特定事業的個人資料處理（包括法人名稱、設立形式及其聯繫方式）。

註 3：歐盟 GDPR 第 4 條第 (7) 款規定：「控管者」係指單獨或與他人共同決定個人資料處理之目的與方法之自然人或法人、公務機關、局處或其他機構；依照歐盟法或會員國法決定處理之目的及方法，由歐盟法或會員國法律規定控管者或其認定之具體標準。

註 4：歐盟 GDPR 第 4 條第 (8) 款規定：「處理者」係指代控管者處理個人資料之自然人或法人、公務機關、局處或其他機構。

註 5：Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive)

註 6：如歐盟 GDPR 第 84 條罰則（Penalties）規定：會員國應制定違反本規則所適用之其他罰則





之規定，尤其係依第 83 條不受行政罰鍰拘束之侵權行為，並應採取一切必要措施確保該等規範得予執行。該罰則應有效、適當且具懲戒性（第 1 項）。各會員國應於 2018 年 5 月 25 日前將其依第 1 項規定通過之法律規定及任何後續影響該等規定之修正案通知執委會，不得遲延（第 2 項）。

註 7：本文使用財團法人金融聯合徵信中心出版之歐盟個人資料保護規則之中文翻譯，資料來源：  
[http://www.jcic.org.tw/main\\_ch/docDetail.aspx?uid=1566&pid=1566&docid=764](http://www.jcic.org.tw/main_ch/docDetail.aspx?uid=1566&pid=1566&docid=764)。

註 8：歐盟 GDPR 第 4 條第(11)款規定，所謂「同意」係指資料主體基於其意思，透過聲明或明確肯定之行動，所為自主性、具體、知情及明確之表示同意處理與其有關之個人資料。

註 9：我國個人資料保護法第 51 條第 2 項規定，公務機關及非公務機關，在中華民國領域外對

中華民國人民個人資料蒐集、處理或利用者，亦適用本法。

註 10：個人資料保護法第 21 條規定：「非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：一、涉及國家重大利益；二、國際條約或協定有特別規定；三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞；四、以迂迴方法向第三國（地區）傳輸個人資料規避本法。」

註 11：個人資料保護法第 12 條規定，公務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。惟金管會指定非公務機關個人資料檔案安全維護辦法第 6 條第 2 項規定，銀行業遇有重大個人資料安全事故者，應即通報金管會。

## 業務報導

- 一、本會於本（107）年 3 月 29 日及 30 日第二度於美國紐約舉辦之「海外分區經理人、法遵人員暨內稽內控研討會」，圓滿竣事，計有 8 家國銀董事長、總經理親率員出席，總計約 120 位參與，交流熱烈，成果豐碩。
- 二、鑒於近年來全球金融監理單位對於新興的金融科技應用投入相關的研究與測試，發展金融沙盒規範，鼓勵金融創新，訂定新的金融法遵條

件，並利用金融科技的數據應用提升對金融犯罪、反資恐、反洗錢的監管技術，本會於 107 年 4 月 16 日委請台灣金融研訓院辦理「國際科技金融論壇 - 金融科技與監理趨勢」，邀請主管機關代表及國際級 FinTech 權威專家與會分享實務洞見，協助銀行瞭解金融科技業務監理趨勢，本活動計有金融從業人員 213 人參加。

## 預告活動訊息

- 一、本會訂於 107 年 6 月 1 日至 11 月 29 日間委託台灣金融研訓院承辦「2018 國際化金融人才培育計畫」，本計畫以育成海外業務開拓管理人才為目標，課程主題涵蓋「法令規範」、「國際視野」、「策略管理」、「業務發展」及「團隊溝通」等五大領域，透過高階決策主管經驗分享、分組個案模擬演練、海外機構考察活動，幫助參訓人員建立國際視野、市場開發經營與產品服務之創新實力。
- 二、本會訂於 107 年 6 月 1 日至 11 月 29 日間與台灣金融研訓院共同主辦「2018 金融高階主管儲訓計畫」，本

計畫以探究金融業經營模式「變革」與「創新」為主軸，架構「策略創新」、「領導發展」、「跨域整合」、「變革執行」四大培訓模組，強化策略創新、跨界整合及變革執行；並訂於 9 月 29 日至 10 月 6 日至法國進行移地訓練與考察參訪，研習內容包含「經營管理」及「金融實務」等相關議題。

三、本會訂於 107 年 5 月 25 日委託台灣金融研訓院承辦「兩岸金融研討會 - 兩岸防制洗錢與打擊資恐」，邀請兩岸產官學界重量級專家共同與會，從金融業監管角度，探討兩岸在監理及洗錢防制法規方面之關注重點，期藉此深化兩岸在金融監理及洗錢防治經驗交流。

四、本會訂於 107 年 6 月 26 日委託台灣金融研訓院承辦「前進亞洲布局論壇」；並自 107 年 6 月 29 日至 9 月 13 日間辦理「亞洲市場人才培訓班」，分別聚焦菲律賓、越南、印尼、緬甸及柬埔寨等 5 個目標市場之政經、金融與產業發展趨勢與人文全貌，邀請熟稔亞洲市場之資深金融專家，從各國政經情勢、金融法規、產業環境、台商經營情況、風俗民情及語言文化等層面，幫助金融業者掌握亞洲市場最新脈動。

五、本會賡續委託台灣金融研訓院承辦「中華民國銀行公會 107 年度開放式影音課程計畫書」，預計於 107 年 6 月至 12 月間，建置上架包括銀行業核心人才 - 國內初階課程、國內進階課程、兩岸金融研討會及前進亞洲佈局論壇等 4 大類共 430 門課程，放置於本會網站供金融從業人員及社會大眾免費使用。