有過必悛—違反個資法的責任與罰則

蔡柏毅／金融聯合徵信中心 法務室

一、前言

法律作為一種規則，通常伴隨強制力，亦即凡違反法律規定的人，將會受到規則所定的制裁，例如喪失權利/利益，或者發生應作為或不作為的義務等等。法律與其他社會生活規範（如道德、習慣等）最大的不同，即在於法律的背後有公權力的強制力。

而在法學上，「法律要件」必須加上「法律效果」才能形成完整的條文結構，缺乏法律效果的法律規定，通常稱之為「訓示規定」，無法直接作為請求他人（或訴諸公權力）為一定作為、或不為特定行為的法律基礎。因此我們可以說，法律規範就是一組條件式規定，由「構成要件」及「法律效果」兩部分組成，在構成要件被滿足的情況下，就發生相對應的法律效果；反之，如果構成要件不成立/不該當，法律效果即無由存在，而法律效果即以強制力作為其執行的保證。

我國個人資料保護法（下稱個資法）以及歐洲聯盟規則第2016/679號一般資料保護規則（General Data Protection Regulation，下稱 GDPR），都是完整而且堪稱成熟的成文法典，自均同時具備「法律要件」與「法律效果」規定。

有關「法律要件」的規定，例如：個人資料的蒐集、處理與利用，原則上均須有法律依據、或有權利主體（當事人）的同意作為基礎[1]；又如：個人資料的蒐集、處理，必須存在具體且適法之「特定目的」，除法律另有規定、或經當事人同意者外，不得為特定目的以外之利用[2]等。

1 可參閱本刊第35期「法規時論」專欄刊載之拙著<你的同意不是我的同意－淺介個資法上的「同意」>。

2 可參閱本刊第37期「法規時論」專欄刊載之拙著<不可須臾離也－淺介個資法帝王條款「目的拘束原則」>。

至於「法律效果」的規定，即為本文討論之主題：違反個資保護相關法規將發生的後果與制裁結果，如何判斷責任的歸屬，分析檢視不同法規範罰則的異同，並簡要介紹具代表性之實際案例。

二、GDPR中與違法責任及罰則相關之條文

摘錄GDPR前言（recitals）及法典本文中與「責任與罰則」相關條文如下：

(一) 前言（148）：

「為強化本規則之執行，對本規則之任何違反，應被處以包括行政罰鍰等處罰，含監管機關依本規則實施之適當措施或其他替代措施在內。

在輕微違規情形，或處以罰鍰將造成對當事人不相當之負擔時，得採用告誡（reprimand）等方式以取代罰鍰。惟仍應就違反之性質、嚴重性、持續期間、是否為故意、有無降低損害之行為（actions taken to mitigate the damage suffered）、責任程度（degree of responsibility）或先前違反之程度、監管機關知悉違法行為後之態度、控管者或處理者所為措施之遵循、對於行為守則之遵守以及任何加重或減輕因素，為相當之考慮。

實施包括行政罰鍰在內之處罰，應遵循歐盟法一般法律原則之正當程序原則保障，包括有效之司法保護及正當程序等。」

(二) 前言（149）：

「會員國得就本規則之違反，包括依本規則規定及在其限制範圍內所定內國法規定之違反，擬定相關刑罰規範。該等刑罰亦得允許沒入因違反本規則所獲之利益。

對該等內國規範之違反所處之刑罰及行政罰，不得違反「一事不再理原則」（ne bis in idem）[3]。」

(三) 前言（150）：

「為強化及協調違反本規則所裁處之行政罰，各監管機關處以行政罰鍰應指出構成違反之事實、行政罰鍰的上限及裁罰基準（upper limit and criteria）等。監管機關應決定並考量個案所有情狀及違反之性質、嚴重性、持續期間及其後果，以確保遵循本規則所定義務而採取相關措施，以預防或減輕該等違反所造成之後果。

對企業處以行政罰時，就企業之定義應遵循歐洲聯盟運作條約第101條及第102條之目的加以理解。

對個人處以行政罰時，監管機關在考量適當之罰鍰金額時，應考量該會員國之平均所得及該個人之經濟狀況。此時一致性機制（consistency mechanism）得被援用，以促進行政罰在適用上之共通性。

會員國得決定是否得對其他公務機關處以行政罰，以及至何程度。

3 又稱「一事不二罰」或「雙重起訴禁止（double jeopardy）」原則，意即任何人均不得因為同一行為而再次受到處罰。原文為拉丁文，於歐盟或大陸法系國家法律條文中通常作為專有名詞，而直接使用原文，不翻譯為英文或其他語言。

處以行政罰或給予告誡，不影響監管機關其他權力之行使，或本規則下其他處罰之實施。」

(四) 前言（152）：

「本規則並未就行政罰鍰定有一致規範，如於具體個案有必要，例如嚴重違反本規則時，會員國應採用有效、適當及懲戒性之處罰措施（effective, proportionate and dissuasive penalties）。至於該等處罰屬刑事或行政性質，則聽由會員國法律決定之。」

(五) 本文第82條「賠償請求權及義務（Right to compensation and liability）」[4]：

1. 因違反本規則而遭受物質上或非物質上之損害時，任何人應有權利自控管者或處理者就其損害獲得賠償。
2. 資料之控管者應對違反本規則之資料處理造成之損害承擔責任。在處理者未遵循本規則所定義務，或其行為超出或違反控管者合法之指示時，處理者應對資料處理造成之損害承擔責任。
3. 若控管者或處理者可證明對於造成損害之事件不可歸責時，得免除第2項規定之責任。
4. 有超過一個控管者或處理者，或控管者和處理者皆同時涉及同一資料處理，且依第2項及第3項對造成損害之資料處理應負責任時，各控管者或處理者對整體損害均負責任，以確保對資料主體有效之賠償。
5. 若控管者或處理者依第4項就損害為全部之賠償，則該控管者或處理者得依照第2項所規定之條件，向其他涉及同一資料處理行為之控管者或處理者請求償還各自就該損害應分擔之部分。
6. 為行使受償之權利而進行之訴訟程序，應向第79條第2項所述會員國法下有管轄權之法院提起之。

(六) 本文第83條「裁處行政罰鍰之一般要件」（General conditions for imposing administrative fines）」：

1. 依本條規定對於違反本規則處以第4項、第5項及第6項所定之行政罰鍰者，各監管機關應確保於個案中係有效、適當且具懲戒性。
2. 依個案情形，行政罰鍰得附加或取代以第58條第2項第a至h點及第j點所定之措施。

於個案中決定是否處以行政罰鍰及決定其數額時，應考慮下列因素：

(a)違規之性質、嚴重性及持續期間（the nature, gravity and duration of the infringement），並考量處理之性質、範圍或目的、受影響之資料主體人數及其受損之程度；

(b)違規之故意或過失（the intentional or negligent character of the infringement）；

4 本條規定與大陸法系民法典所定「侵權行為損害賠償」之原理原則高度相近，例如「非財產上損害賠償」（第1項）、「特殊類型之侵權行為」（第2項）、「歸責原則之認定」（第3項）、「共同侵權行為責任」（第4項）、「責任分擔與內部求償」（第5項）等。

(c)控管者或處理者所採用而有效減少資料主體損害（mitigate the damage suffered by data subjects）之任何行為；

(d)控管者或處理者之責任程度，並應考量其依第25條及第32條所實施之技術上及組織上措施；

(e)控管者或處理者先前任何相關之違規情事；

(f)與監管機關之配合程度，以糾正或減輕其違規所可能造成之不利影響；

(g)違規所影響之個人資料類型；

(h)監管機關知悉其違規之方式，尤其是控管者或處理者是否依規定通報該違規，或其通知之程度；

(i)已依照第58條第2項規定命控管者或處理者就同一標的採取相關措施者，該等措施之遵循程度；

(j)第40條所定行為準則或依第42條所定經核准之認證機制之遵循；及

(k)任何其他適用於該個案情形之加重或減輕因素（aggravating or mitigating factor），例如因違規而直接或間接獲得之經濟利益或避免之損失。

3. 對於相同或相關之處理作業，如控管者或處理者因故意或過失違反本規則之數個規定者，行政罰鍰總額不得超過最嚴重違規情事所定之數額。

4. 依照第二項規定，違反下列規定者，最高處以10,000,000歐元之行政罰鍰，如為企業，最高可達前一會計年度該企業全球年營業額之百分之二，兩者以較高者為準：

(a) 第8條、第11條、第25條至第39條及第42條及第43條所定控管者及處理者之義務；

(b) 第42條及第43條所定認證機構之義務；

(c) 第41條第4項所定監管機關之義務。

5. 依照第二項規定，違反下列規定者，最高處以20,000,000歐元之行政罰鍰，如為企業，最高可達前一會計年度該企業全球年營業額之百分之四，兩者以較高者為準[5]：

(a) 第5條、第6條、第7條及第9條所定處理之基本原則，包括同意之條件；

(b) 第12至22條所定資料主體之權利；

(c) 第44條至第49條所定個人資料移轉至第三國或國際組織之接收者；

(d) 依照第9章規定通過之會員國法律所定之任何義務；

(e) 違反監管機關依第58條第2項規定之命令或暫時性或終局性之處理限制或停止資料傳輸，或違反第58條第1項規定。

6. 違反監管機關依第58條第2項規定之命令者，依照本條第2項規定，最高處以20,000,000歐元之行政罰鍰。如為企業，最高可達前一會計年度該企業全球年營業額之百分之四，兩者以較高者為準。

5 此處GDPR第83條第5項規定所列5款違反規則情事，以及第5項有關違反監管機關依規定之命令者，其涉及的範圍極廣，罰鍰亦復極重，概為GDPR之所以被稱為「史上最嚴格個資法」的主要原因之一。尤其「跨國企業前一會計年度全球營業額之一定百分比」之裁罰基準設計，對企業年度獲利的負面影響程度至鉅，已足以引起高度注意與討論，尤其對於有遭受此處罰可能性的國際性公司，肯定會引發其股東與董事會的極度關注。

7. 在不損及監管機關依第58條第2項所定糾正權力之情況下，會員國得制定是否及如何對設立於該會員國之公務機關及機構處以行政罰之規定。
8. 監管機關依本條規定執行時，應遵守歐盟法及會員國法律，採取適當程序保障，包括有效之司法救濟及正當程序等。
9. 如會員國之法律體系未規定行政罰鍰，而該體系已確保有效之司法救濟且監管機關所裁處之行政罰鍰具有相同效力者，本條規定得由監管機關裁處之，並由該國國內管轄法院執行。

該等罰鍰應有效、適當且具懲戒性。

各會員國應於2018年5月25日前，將其依本規定通過之法律通知（歐盟）執委會，任何後續之修法或影響該等規定之修正案，亦同。

三、違反GDPR的責任要件與判斷基準

GDPR第83條第2項列出了在具體個案中，是否處以行政罰款以及決定具體的罰款數額時應當考慮的11款評估標準。其中有關「違規行為的性質」部分，引進「輕微侵權」（minor Infringement）概念，如果監管機關認為該違規行為不會對資料主體的權利構成重大風險，則可以告誡方式取代。

有關違規行為的持續時間部分，因侵害個人資料行為通常有難以確定及控制的性質，因此在計算違規行為截止時點，可以藉由是否為故意行為（故意行為有明知及意欲等主觀要件，其時點判斷較為明確）、是否未採取適當的科技化且有組織的預防或處理措施等，協助判斷違規行為是否還在持續狀態。

有關違規行為對資料主體帶來的風險及損害部分，判斷損害之重大性判準如：歧視行為；身份盜用（identity theft）或詐騙行為；鉅額財產損失；有關名譽等非財產上之損害；本法所定特殊性質個人資料被任意公開；未經授權即移除加密或假名化處理（pseudonymisation）；使資料主體喪失對其個人資料的權利和自由，無法充分行使控制權；為建檔（profiling）目的而分析或處理個人資料，尤其對經濟狀況、健康狀況、工作表現、信用評價、個人偏好或興趣、常態性活動或其地點進行分析和預測；對未成年人資料的處理；蒐集或處理行為涉及的個人資料及影響的資料主體數量龐大等情形。

有關違規行為是否出於故意或過失部分，因基於故意的違規行為比過失更具可非難性，更有可能應該處以行政罰款。在個案中的「故意」行為，可能有以下幾種：由最高管理階層明確授權進行的資料處理；不顧監管機關的建議、或無視已頒布之政策而違規之行為；對個人資料進行惡意的竄改，企圖達到誤導性效果等等。至於「過失」行為，可能包括：未能閱讀及遵守相關規定（近乎純粹不知法律）；因人為錯誤漏未檢查相關個人資料之正確性；未及時更新科技上、組織上的預防措施與技術等，惟「資源短缺」並不得作為合理化違規行為的藉口。

有關控管者或處理者為減輕資料主體遭受的損害而採取的補救措施部分，當發生違規行為並且對資料主體帶來損害時，應盡一切可能降低對資料主體的不利影響。監管機關在考量裁罰時，很大程度上會考慮責任方是否採取了補救措施，作為決定採用何種處罰以及處罰程度的衡量因素，對於事後明確承認其違法，並負責的糾正其行為影響的控管者或處理者，更有可能獲得從寬處理。

有關控管者或處理者的責任程度部分，GDPR基於課責原則（accountability），要求行為人確實遵守個人資料處理的基本原則，並就符合相關原則負舉證之責。評估控管者或處理者的責任程度方式包括：是否實施設計與預設（by design and by default）資料保護原則等技術上措施、是否採取有關資料保護之組織上措施、有關資料保護之政策是否被各級資料的控管者及處理者確實知曉與應用等。

有關控管者或處理者相關違規行為部分，該判準旨在評估先前的違規行為，包含責任主體可能存在及正在接受調查的其他違規行為，以綜合判斷該責任主體究屬單純對規則瞭解不足，或屬對規則的輕視與無視。

有關與監管機關配合的程度部分，配合執法措施本為義務，因此並非所有的配合行為都能成為從寬處理的事由，而必須在案件的調查階段，對監管機關相關舉措都能積極配合，並儘其所能減輕對資料主體遭受的損害，方屬之。

有關受違規行為影響的個人資料的類別部分，主要針對敏感、特殊、容易被侵害、或受損害風險較高的個人資料，提高其保護要求，包括是否涉及處理特殊類型之個人資料、是否得以直接或間接識別特定資料主體、是否對資料主體造成直接侵害上損失、資料是否受有相關技術保護、或是否採取加密措施等。

有關監管機關知悉違規行為的方式部分，監管機關可能以包括調查、舉發、投訴、報導、或因控管者的通知而獲知相關情況等，惟依GDPR第32條之規定，個人資料侵害應於發現後 72 小時內通報監管機關，不得無故稽延，因此當控管者僅僅履行此義務時，對該義務的遵守尚不能直接作為減輕責任之事由。

有關控管者或處理者對相關措施的遵循部分，監管機關依GDPR第58條第2款對控管者或處理者作出相關命令或措施後，對相關措施的遵守情況，亦為判斷責任程度輕重之標準。

有關對GDPR第40條行為準則與GDPR第43條規範之認證機制的遵守部分，當控管者或處理者表明遵循行為準則或經核准之認證機制時，該認證機構得採取相關監督措施，監管機關得認可此類措施的有效性，而暫不採取其他裁罰措施。

有關其他加重或減輕因素部分，旨在依個案考量，以作出更合適的處罰措施，其範圍較為廣泛，前揭10款判準之外的其他因素都包含在內，而係概括規定。因罰款之主要性質為對責任主體的經濟狀況施以制裁，故「因違規行為而直接或間接獲得的經濟利益、或得以避免之損失」尤為重要之考量因素。

四、GDPR三週年－裁罰案例統計分析

歐盟自2018年5月25日開始正式實施GDPR，截至本文撰稿日（2021年6月）已施行屆滿三年，據非官方統計[6]，歐盟境內各會員國個資保護當局依GDPR 裁處行政罰鍰的案例已超過 16 萬筆，累積之罰款金額逾2.6億歐元（約折合3.1億美元或新臺幣87億元）[7]。

以國別統計，義大利為罰款總額最高國家，其次是法國及德國；裁罰個案之數量方面，以西班牙總件數最多，其次是義大利及羅馬尼亞；至於平均每案罰款（以罰款總額除以裁罰個案數量）部分，最高則為英國，其次是德國與瑞典。

歷年來因違反GDPR規定而被裁處罰鍰的案例中，罰款數額最高且具代表性之案例，厥為法國個資保護監管機關，即法國「國家資訊與自由委員會」（Commission Nationale de l'informatique et des Libertés, CNIL）於2019年1月間裁罰跨國科技巨擘Google 公司5000萬歐元一案（以下簡稱「本案」）[8]。

「法規時論」專欄前曾為文介紹歐盟法院（Court of Justice of the European Union）於2014年5月，針對當事人「被遺忘權」的請求，所作出的 "Google Spain v. AEPD案判決。該案Google敗訴，必須移除原告在搜尋引擎上的相關資料與搜尋結果。惟當時GDPR尚未實施，依當時有效之「歐盟個人資料保護指令」（Directive EU 95/46/EC）第24條有關罰則之綱領性質規定，須待各會員國制定個資保護相關法律，始能納入行政罰鍰[9]，與本案情形有所不同。

分析本案主要的裁罰理由，主要是CNIL認為Google 未能提供使用者足夠的透明性，並且未能取得使用者的有效同意[10]，因此未能符合GDPR有關當事人資訊自主的規定，爰參酌違規性質的普遍性及侵害嚴重程度，對Google祭出鉅額罰款。據前述行政罰鍰統計，GDPR施行三年來共裁罰2.6億歐元，本案以一案即佔罰款總數近20%。究其原因，一方面係依GDPR第83條第5項規定，以Google前一會計年度全球年營業額為計算基準，其母數龐大[11]；另方面，以Google搜尋在個人電腦平臺，

6 CMS.LAW, GDPR Enforcement Tracker：https://www.enforcementtracker.com/?insights。CMS是一間總部位於倫敦的跨國法律事務所，持續而長期的追蹤並公開GDPR在歐盟各國、各業別、違規類別的裁罰情形，並彙整出版年度報告，最新版為”GDPR Enforcement Tracker Report-2021”。本文所引述之統計數據以此年度報告及網站揭載資料為主。

7 並非所有歐盟成員國依各自所訂規範都完整公開違反 GDPR 相關的統計數據，或有部分成員國僅提供部分或尚未公開最近年度之最新數據，因此實際案例數量及罰款金額應比統計值更高。

8 CNIL官網新聞稿，網址連結（最後瀏覽日：2021/6/10）：https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc。

9 可參閱本刊第34期「法規時論」專欄刊載之拙著<不如相忘於江湖－淺介「被遺忘權」與「刪除權」>。

10 GDPR對「當事人同意」之有效性有嚴格的規範，可參閱同註1拙著。

11 該條項規定之罰鍰最高僅為2,000萬歐元，或全球營業額的4%，因此本案CNIL明顯是以後者來計算罰鍰數額。

以及旗下Android 作業系統在智慧型手機平臺的普遍重要地位，幾乎只要使用資訊產品，就很有可能成為Google的用戶，影響層面極其廣泛，因此本案在具有各方面之高度代表性與象徵性，堪稱GDPR研究之指標性案例（leading case）之一。

本案最初肇因有倡議團體[12]抗議Google運用使用者的個人資料發送「個人化廣告」（ads personalization），認為Google提供的資訊與說明並不容易讓使用者取得及理解，包括取得資訊的用途、儲存期間等重要資訊，均散見於多個文件的各處，有意瞭解者須一再點選按鍵及連結才能完整取得。再者，Google提供的資訊網路服務種類繁多，如youtube隨選影音服務或Googlemaps網路地圖服務等不同來源的資訊，於分散式蒐集後，卻集中經由自動分析建檔合併，進行分析及處理，因而得以大量、廣泛卻精準的，取得個別用戶的喜好等相關特徵資訊，用於推送高度個人化之廣告訊息。

Google於本案抗辯表示，其係取得用戶同意後，才針對相關資料進行處理及作為發送廣告之利用，並且有提供用戶修改與帳戶關連的選項。惟 CNIL 認為，使用者於註冊帳戶時如不被動接受廣告，即無法取得服務[13]，且於帳戶建立後，必須到「更多選項」去調整相關設定，如未另行變更設定，即預設同意顯示個人化廣告，違反GDPR第4條：「同意必須自主作成（freely given）、具體（specific）、受充分告知（informed）且為非模糊（unambiguous）之明確而肯定的行動（clear affirmative act）」，以及「預設為同意之選項（pre-ticked boxes）或單純不為表示（inactivity），均不構成同意」等規定。

此外，CNIL認為Google並未依規定，提供充分而完整的說明及相關資訊予使用者，包括蒐集個資進行處理的目的、資料儲存的期間、有那些種類個資將被利用（或不被利用）於個人化廣告行為上等重要訊息，均散見於不同的網頁文件及連結中，使用者無法輕易而直覺的取得完整的資訊。

至於本案罰鍰的計算方式部分，CNIL指出，Google 是「持續性、長時間、大範圍」的違反GDPR規定，且Google 公司的獲利模式本就側重廣告，因此在本案中嚴格檢視其與「個人化廣告」相關的蒐集、處理與利用的要件是否合致，即屬當然，而且必須。再者，本案裁罰目的在於要求 Google 應讓用戶得以充分控制自己的資料，先完整告知用戶相關的資訊與風險，並取得用戶的有效同意，始與GDPR規定相符。綜合以上所述，CNIL認為本案罰鍰數額尚稱合理。

12 此二個團體分別為None Of Your Business（“NOYB”）和 La Quadrature du Net（“LQDN”）。
13 一般稱之為「綑綁式同意」（bundling consent），並非有效同意。

除本案外，統計「平均每案裁罰數額」最高的英國[14]，其個資保護監管機關，即英國「資訊專員辦公室」（Information Commissioner's Office, ICO）於2019年7月，就兩起重大的駭客入侵造成大量用戶個資洩漏案件，對英國航空（British Airways, BA）及萬豪（Marriott）國際酒店集團，最終分別裁罰2000萬英鎊及1840萬英鎊[15]。ICO認為，由於二間企業缺乏適當的資安機制，才讓駭客有機可趁，實已違反GDPR第32條有關資料控管及處理者應採取適當科技化與組織化措施，確保系統及服務持續之機密性、完整性、可用性與彈性之規範義務。

至於GDPR目前第二高的罰鍰紀錄，為德國漢堡個資保護監管機關，即該州「資料保護與資訊自由委員會」（Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Hmb BfDI）2019年7月，對時裝公司H&M裁罰3530萬歐元一案[16]。該公司透過對員工非正式約談等方式，蒐集員工的健康狀況、就醫紀錄、家庭狀況、宗教信仰、度假經歷等個人資料，甚至以錄音方式作成詳細紀錄，並以數位方式併同員工檔案長期保存，供各級主管參閱，被使用於評估員工表現，甚至用以決定員工相關管理措施等。BfDI認為，該等監控行為構成對員工個人資料與隱私的強烈侵犯，有關資料之蒐集、處理與利用均缺乏GDPR規定之依據，具高度之可非難性，惟該公司於事件發生後明確承認其違法行為，並已採取相關補救措施，例如管理階層不僅向受到影響的員工公開道歉，並向員工支付了為數可觀的損害賠償金等，因此「罰款金額已足以阻止該公司未來繼續侵犯其員工的隱私。」[17]

義大利雖為GDPR罰款總額最高及裁罰個案數量第二高之國家，其主要裁罰對象有較集中的現象，例如TIM Group遭處2780萬歐元、Wind Tre S.p.A.遭處1670萬歐元、Vodafone Italia S.p.A.遭處1225萬歐元等，均屬資訊、通訊、網路產業因違反GDPR而受罰之案例。

五、我國個資法上責任及罰則相關規定

我國個資法為規範個人資料保護之單行法規，違反個資法之規定，可能發生民事責任、刑事責任與行政責任：

14 英國於2020年1月31日正式退出歐盟前，仍直接適用ＧＤＰＲ。

15 ICO原本作出的裁罰數額計算方式，是以全年營收的1.5%計算，BA的罰緩高達1.83億英鎊，萬豪則為9900萬英鎊，如果照原定數額計罰，將超過本文提及的Google案5000萬歐元，成為GDPR罰款數額最高及第二高的案例。惟ICO於2020年10月同意大幅度刪減罰緩，理由是二家企業於案發之後相關改善措施的表現良好，以及為了因應COVID-19疫情對經濟所帶來的衝擊。可參閱ICO官網發布之相關新聞稿，網址連結（最後瀏覽日：2021/6/10）： https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/及https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/。

16 歐洲資料保護委員會（European Data Protection Board, EDPB）就本案發布之新聞稿，網址連結（最後瀏覽日：2021/6/10）：https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en。

17 引述Hmb BfDI 專員Prof. Dr. Johannes Caspar於同前註新聞稿中的評述。

(一) 民事責任

1. 公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。（個資法第28條第1項規定參照） 必須因天災、事變或不可抗力所致者，始能免除責任，學理上稱為「事變責任」，責任程度較重。
2. 非公務機關違反個資法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。（個資法第29條第1項規定參照） 因以有故意或過失為責任條件，學理上稱為「過失責任主義」，責任程度較公務機關為輕。
3. 對於基於同一原因事實應對多數當事人負損害賠償責任之總額，上限為新臺幣（下同）2億元[18]，被害人不易或不能證明其實際損害額時，得請求法院依侵害情節以每人每一事件500元以上2萬元以下計算（個資法第28條第3項、第4項規定及第29條第2項規定參照）。惟當事人得以證明之損害均得請求賠償，如個資法規範有不足者，仍得依民法相關規定請求。因此個資法有關每人、每一事件賠償金額上、下限之規範，僅於不易或不能證明其實際損害額之情形時，始有必要。

(二) 刑事責任

意圖為自己或第三人不法之利益或損害他人之利益，違法蒐集、處理或利用個人資料者；或對於個人資料檔案為非法變更、刪除、或以其他非法方法，妨害個人資料檔案之正確，而足生損害於他人者，均課予刑事責任，並得併科100萬元以下之罰金。（個資法第41條、第42條規定參照）

(三) 行政責任

非公務機關違法蒐集、處理或利用個人資料者，依其違規程度，由中央目的事業主管機關或直轄市、縣市政府處以2萬元以上20萬元以下，最高為5萬元以上50萬元以下之罰鍰，並令限期改正，屆期未改正者，並得按次處罰。此外，非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前述規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰，以加重其監督之責任。（個資法第47條至第50條規定參照）

是以依我國個資法規定，對於同一違規事件，最高之行政罰鍰金額，處罰非公務機關部分為50萬元，處罰其代表人、管理人或其他有代表權人部分亦為50萬元，二者合計僅為100萬元，惟有未於期限內改正者，得按次連續處罰之規定。

18 1995年頒行的「電腦處理個人資料保護法」（現行個資法修正前舊法），此處賠償總額之上限為2000萬元，現行個資法於2012年施行後已提高10倍至2億元。

六、結論

GDPR作為一個超國界之個資保護法規，就違規之刑事責任部分，悉交由各會員國制訂，僅就其有效性、適當性及懲戒性部分作綱領性規範[19]；在民事責任部分，則基於「有損害即有賠償」之法理，與民法侵權行為損害賠償責任重合[20]；惟在行政責任方面，就事實之認定、行政罰之裁罰基準、責任要件、以及執行上之一致性等等，則有較為完整之規定。

我國現行個資法於2010年公布之修正說明以：「……現今公務機關或非公務機關蒐集、處理、利用或國際傳輸個人資料之情形日漸普遍，為加重個人資料蒐集者或持有者之責任，促其重視維護個人資料檔案安全之措施，並使被害人能受到較高額度之賠償，…且總額限制之金額過低時，恐將產生實務操作之困難，爰…將賠償總額提高。」前揭文字敘述提高部分雖為民事賠償責任，惟其敘述之事實於10年後今日之時空背景不但仍有適用，情況恐怕只有更為嚴峻。

在網路資料快速流動而且倍速成長的當代，對於個人資料之侵害程度，如以蒐集、處理、利用或國際傳輸個人資料的規模、範圍及期間加以衡量，跨國企業或組織的影響層面恐更為廣泛，且為我國現行個資法規範下，較不易有效處理的部分。因此GDPR中有關高額之行政罰鍰，以及嚴格而有效之罰鍰計算方式部分，以及3年來的實際執行案例，應有值得我國個資法制借鑒之處。

參考文獻：

1. 尤重道，個人資料保護之概念與蒐集處理利用暨違法責任，全國律師，21卷8期，2017年8月。
2. Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP253, last Retrieved on 2021/06/10, from https://ec.europa.eu/newsroom/article29/items/611237.

19 GDPR前言（149）及（152）參照。

20 GDPR本文第82條參照。就我國個資法以數條篇幅規範之團體訴訟部分，GDPR雖無相關規定，惟實務上仍得依民事訴訟程序或消費者保護相關程序執行之。