

「歐盟、南韓、新加坡個人資料保護法對於違反安全維護義務之行政處罰規定」委託研究計畫

結案報告

委託機關：國家發展委員會

受託單位：達文西個資暨高科技法律事務所

中華民國 112 年 5 月

「歐盟、南韓、新加坡個人資料保護法對於違反安
全維護義務之行政處罰規定」委託研究計畫
結案報告

受託單位：達文西個資暨高科技法律事務所

計畫主持人：葉奇鑫

計畫期程：中華民國 112 年 4 月至 112 年 5 月

國家發展委員會 委託研究

中華民國 112 年 5 月

本研究報告內容僅供本會業務參考

摘要

隨著數位時代之發展，人民對個資保護之意識與需求逐漸提升，透過法規調適強化個資保護並兼顧個資合理運用，已成為各國政府面對之重要課題。罰則規範可嚇阻違法行為、促進個人資料保護法規之遵循，是各國法規調適過程中的重要議題之一，其中，行政罰鍰因其靈活、快速等特性，逐漸成為各國個人資料保護法(下稱個資法)執法制度之重心。在此方面，歐盟、新加坡、南韓等先進國家皆相繼採行立法或修法措施，導入雙軌制高額行政罰鍰制度，作為個資法有效落實之保障。

我國個資法於 112 年 5 月修正，提高第 48 條個資安全維護不足之罰則，以回應社會各界關於強化業者個資保護作為之期待。此外，後續由個人資料保護委員會研擬第二階段個資法全面修正。屆時，個資法第 47 條至第 49 條之罰鍰規範，仍將是修正的重點之一。如何在個資法後續修正中，回應社會及民眾之期待、促進個資法之有效落實、減緩對產業之衝擊，並提升我國與國際法制之一致性，即有深入研究之必要。因此，本研究受國家發展委員會委託，對先進國家個人資料保護法制中行政罰鍰規範、實務運作標準、裁罰案例等作比較分析，研擬我國個資法罰鍰規範調整方向建議，並提供修法條文草案，供作我國修法作業之參考。

Abstract

Along with the advance of the digital age, people's awareness and demand of personal data protection is arising. Amendment of existing laws in a way that enhances data protection while also encourages the proper use of data has become a major task for governments around the world. Penalty provisions can deter infringements and promote compliance, making them a key issue in the law-amendment process. In particular, administrative fines is becoming the center of data protection law enforcement regimes, due to their flexibility and efficiency. In this respect, the European Union, Singapore and South Korea have all adopted legislative measures that introduce a dual-track administrative fine system with a high upper limit, as a guarantee for effective enforcement of the data protection law.

Taiwan has completed the amendment of its Personal Data Protection Act (PDPA) in May 2023, which, in response to society's expectations for enhanced data protection by businesses, specifically increases penalty for insufficient security safeguards under Article 48. In the meanwhile, competent authorities are also in the process of formulating a further, comprehensive amendment to the PDPA, with Articles 47 to 49 on administrative fines remaining a main issue. In order to meet the expectations of society, contribute to effective enforcement of the PDPA, mitigate the potential impact on industries, and align Taiwan's level of data protection level with the international standard, the National Development Council (NDC) has commissioned this research to conduct a comparative study of the rules, practical standards and cases of leading countries on administrative fines for data protection violations, so as to draw reference for Taiwan's amendment of the PDPA and formulate a draft proposal on the amended provisions.

目錄

第一章	研究目的.....	1
第二章	研究方法.....	3
第三章	外國法規研析.....	5
第一節	歐盟.....	5
一、	規範重點.....	5
(一)	法規內容要點.....	5
(二)	法規立法理由.....	10
(三)	實務運作標準.....	10
(四)	案例.....	31
二、	簡析.....	43
第二節	新加坡.....	45
一、	規範重點.....	45
(一)	法規內容要點.....	45
(二)	法規立法理由.....	49
(三)	實務運作標準.....	53
(四)	案例.....	60
二、	簡析.....	63
第三節	南韓.....	64
一、	規範重點.....	64
(一)	法規內容要點.....	64
(二)	法規立法理由.....	69
(三)	實務運作標準.....	70
(四)	案例.....	83

二、 簡析	88
第四章 針對我國之建議.....	95
第一節 我國法制中的雙規制裁罰上限	95
一、 公平會規範重點	95
(一) 浮動上限之適用範圍	95
(二) 罰鍰之計算方式	97
二、 實務運作案例	99
第二節 比較分析	100
一、 雙軌裁罰制度之整體設計	100
(一) 雙軌制之罰鍰金額	101
(二) 雙軌制罰鍰之適用	106
二、 罰鍰之計算方法	109
(一) 計算步驟	109
(二) 罰鍰金額之計算基礎	109
(三) 加重或減輕事由	111
第三節 針對我國具體建議	112
(一) 罰鍰制度之整體設計	112
(二) 浮動罰鍰上限之導入	117
(三) 配套措施	121
(四) 修法條文草案	123
第五章 結論	128
參考文獻	131

表目錄

表 1	行政罰鍰相關修正條文草案對照表	124
-----	-----------------------	-----

第一章 研究目的

隨著數位時代之發展，人民對個資保護之意識與需求逐漸提升，透過法規調適強化個資保護並兼顧個資合理運用，已成為各國政府面對之重要課題。罰則規範可嚇阻違法行為、促進個資保護法規之遵循，是各國法規調適過程中的重要議題之一，其中，行政罰鍰因其靈活、快速等特性，逐漸成為各國個資法執法制度之重心。

歐盟於 2016 年訂定、2018 年施行之《一般資料保護規則》(General Data Protection Regulation, GDPR)，採行雙軌制高額行政罰鍰制度，違法行為最高可處 2000 萬歐元罰鍰、或上一年度全球營業額之 4%，以兩者中較高者為準。在此之後，新加坡、澳洲、南韓等國家，亦相繼修正個資法裁罰規範，大幅提高行政罰鍰上限、或導入以營業額之特定比例計算罰鍰之方式¹。

我國在 1995 年《電腦處理個人資料保護法》基礎上，於 2000 年制定《個人資料保護法》（以下稱我國個資法），並於 2014 年進行首次修正後，目前已在研擬該法第二次修正。其中，我國個資法第 47 條至第 49 條之罰鍰規範，是本次修正的重點之一。如何在個資法本輪修正中，回應社會及民眾之期待、促進個資法之有效落實、減緩對產業之衝擊，並提升我國與國際法制之一致性，即有深入研究之必要。

¹ See, Singapore Personal Data Protection (Amendment) Act 2020, <https://sso.agc.gov.sg/Acts-Supp/40-2020/Published/20201210170000?DocDate=20201210170000>; Australian Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022, <https://www.legislation.gov.au/Details/C2022A00083>; 개인정보 보호법 전면개정, 데이터 신경제 시대 열린다, <https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=8674>.

因此，本研究受本研究所國家發展委員會委託，對先進國家個資保護法制中行政罰鍰規範、實務運作標準、裁罰案例等作比較分析，研擬我國個資法罰鍰規範調整方向建議，並提供修法條文草案，供作我國修法作業之參考。

第二章 研究方法

本研究將以文獻分析法為原則，就先進國家個資保護法制中雙軌制行政罰鍰規範之內容作重點摘要，研析其立法理由、實務運作標準及實務案例，歸納其規範模式特徵。此外，本研究亦將以法規比較法，分析先進國家規範模式之異同，並與我國法中既有之雙軌制裁罰規範作比較，提出符合我國社會需求之個資法修法建議。

本研究所比較之國家法律及實務指引如下：

（一）歐盟

歐盟一般資料保護規則（GDPR）第 83 條係關於行政罰鍰之規範。此外，歐洲個人資料保護委員會（European Data Protection Board, EDPB）作為歐盟層級 GDPR 解釋機關，於 2022 年 5 月公布《依 GDPR 計算行政罰鍰之指引 04/2022》（Guidelines 04/2022 on the calculation of administrative fines under the GDPR，以下稱 EDPB 指引）²，針對 GDPR 行政罰鍰之計算提出統一之方法與步驟。

（二）新加坡

2020 年 11 月，新加坡通過《2020 年個人資料保護（修正）法》（Personal Data Protection (Amendment) Act 2020），對《個人資料保護法》（Personal Data Protection Act, PDPA）作出大規模修正，包括增訂 PDPA 第 48J 條，重構行政罰鍰規範。

² EDPB, Guidelines 04/2022 on the calculation of administrative fines under the GDPR (12 May 2022), https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf.

因應 PDPA 之修正，新加坡個人資料保護委員會（Personal Data Protection Commission, PDPC）針對其對 PDPA 相關條文之解釋以及執法策略，訂定《執行資料保護規範之諮詢指引》（Advisory Guidelines on Enforcement of Data Protection Provisions，以下稱執法諮詢指引）³，以及《積極執法指引》（Guide on Active Enforcement）⁴。

（三）南韓

南韓國會於 2020 年 1 月大幅修正其《個人情報保護法》（개인정보 보호법），確立該法作為個資保護普通法之地位。該法第 28 條之 6、34 條之 2 和第 39 條之 15 分別針對不同違法行為，規定不同行政罰鍰額度。此外，《個人情報保護法施行令》就行政罰鍰之計算方式與步驟作出細部規範。

2023 年 2 月，南韓國會通過《個人情報保護法》修正案，增訂第 64 條之 2 規定，強化個資法對經濟上之處罰。該修正案定於 2023 年 9 月 15 日施行。

³ Advisory Guidelines on Enforcement of Data Protection Provisions (October 2022), <https://www.pdpc.gov.sg/guidelines-and-consultation/2020/02/advisory-guidelines-on-enforcement-of-data-protection-provisions>.

⁴ Guide on Active Enforcement (October 2022), <https://www.pdpc.gov.sg/help-and-resources/2019/05/guide-on-active-enforcement>.

第三章 外國法規研析

第一節 歐盟

一、規範重點

(一) 法規內容要點

1. 主管機關科處裁罰之權力

科處行政罰鍰是歐盟個資法主管機關之權力之一。依 GDPR 第 58 條第 2 項，主管機關有權對違反 GDPR 之行為進行糾正，包括：

- (1) 科處行政罰鍰（第 58 條第 2 項第 i 款）；
- (2) 向控管者或受託運用者發布各項命令，包括命令臨時或永久限制個資運用，命令停止資料傳輸，命令遵循 GDPR 等（第 58 條第 2 項第 c 款至第 g 款、第 j 款）；
- (3) 認為控管者或受託運用者擬進行之個資運用活動可能違反 GDPR 時，向其發布警告（第 58 條第 2 項第 a 款）；
- (4) 控管者或受託運用者之個資運用活動違反 GDPR 時，向其發布告誡（第 58 條第 2 項第 b 款）；
- (5) 撤銷認證，或命令認證機構撤銷或拒絕授予認證（第 58 條第 2 項第 h 款）。

依第 58 條第 2 項第 i 款與第 83 條第 2 項本文前段，主管機關視個案情形，得單獨科處行政罰鍰，亦得與其他糾正措施一併科處。

2. 行政罰鍰之金額標準

GDPR 並未就行政罰鍰訂定下限，但依違法行為之內容及所涉條款，規定罰鍰金額之不同上限。以下依裁罰之相對人、所涉條款及規範內容分別說明。

(1) 依第 83 條第 4 項，若違反下列規範，最高可處 1000 萬歐元之裁罰；但違反者若為事業（undertaking），則最高可處相當於前一會計年度全球營業額 2% 之裁罰（以較高者為準）：

(a) 個資運用之控管者或受託運用者：

- 第 8 條關於「資訊社會服務所涉兒童同意」之義務；
- 第 11 條關於「無須識別之運用」之義務；
- 第 25 條至第 39 條規定之控管者及受託運用者的各項義務，包括資料保護設計（by design）與預設（by default）、共同控管者義務、非歐盟控管者或受託運用者在歐盟境內指定代表之義務、控管者對受託運用者之監督義務、受託運用者遵守 GDPR 及控管者指示之義務、紀錄保持義務、向主管機關提供配合之義務、個資安全維護義務、個資侵害事故通知及通報義務、個資影響評估義務、設置個資保護長義務等。
- 依第 42 條及第 43 條所稱認證機制應負之義務。

(b) 認證機構（certification body）：

- GDPR 第 42 條及第 43 條所定之認證機構義務。

(c) 監督機構（monitoring body）：

- GDPR 第 41 條第 4 項所定之監督機構義務。

(2) 依第 83 條第 5 項和第 6 項，若違反下列規範，最高可處 2000 萬歐元之裁罰；但違反者若為事業，則最高可處相當於前一會計年度全球營業額 4% 之裁罰（以較高者為準）：

(a) 個資運用之控管者或受託運用者：

- 第 5 條（個資運用原則）、第 6 條（運用之法律依據）、第 7 條（同意之條件）及第 9 條（特種個資運用）規定之個資運用基本原則，包括同意之條件；
- 第 12 條至第 22 條所規定之個資當事人權利，包括告知義務、近用權、更正權、刪除權、限制處理權、資料可攜權、拒絕權、不受自動化決策拘束之權利等；
- 第 44 條至第 49 條所關於個資境外傳輸之規範；
- 違反主管機關依第 58 條第 2 項所為之臨時或永久限制運用或停止資料傳輸之命令，或拒絕主管機關依第 58 條第 1 項進入其場所或存取其資料運用裝置。
- 違反主管機關依第 58 條第 2 項所為之命令，包括命令滿足個資當事人之權利行使請求，命令遵循 GDPR 之規定，命令向個資當事人通知個資侵害事故，命令更正、刪除或限制運用個人資料等。

(b) 認證機構：

- 未遵循主管機關依第 58 條第 2 項所為之撤銷認證或拒絕授予認證之命令。

(3)依第 83 條第 7 項，對於公務機關或機構之違法行為，會員國在不影響主管機關命令糾正之權力的前提下，得就可否及如何針對公務機關或機構科處罰鍰另定規範。

3. 個案裁罰金額之確定

(1) 考量要素

GDPR 第 83 條第 2 項規定，主管機關須針對個案情形，綜合考量各項因素，決定適當之裁罰金額。該項進而以第 a 款至第 j 款例示 10 項考量要素，並以第 k 款為考量要素之概括條款，各項考量要素包括：

- (a) 違法行為之性質、重大性及持續期間（考量所涉運用作業之性質範圍或目的、所涉個資當事人人數及其所受損害之程度等）；
- (b) 違法行為之故意或過失性質；
- (c) 控管者或受託運用者為減輕個資當事人損害而採取之措施；
- (d) 控管者或受託運用者之責任程度（考量所採取之安全維護措施）；
- (e) 控管者或受託運用者此前之違反情事；
- (f) 控管者或受託運用者為糾正違法行為、減輕不利影響而與主管機關之配合程度；
- (g) 違法行為所涉之個資類別；
- (h) 主管機關知悉違法行為之方式，特別是控管者或受託運用者之通報狀況；

- (i) 若主管機關先前曾就同一標的科處糾正措施，控管者或受託運用者對該措施之遵循狀況；
- (j) 對 GDPR 第 40 條行為守則或第 42 條認證機制之遵循狀況；
- (k) 其他加重或減輕事由，例如因違法行為直接或間接所獲利益、所避免之損失等。

(2) 罰鍰金額之妥適性

為落實行政裁罰之目的，依 GDPR 第 83 條第 1 項，主管機關於個案中所科處之裁罰金額，須具備有效性、合比例性與嚇阻性（dissuasive）。

4. 罰鍰之競合

GDPR 第 83 條第 3 項係關於競合之規範。依該項規定，若同一或彼此關聯之一組運用作業（the same or linked processing operations）違反 GDPR 之數項規範，則行政罰鍰之總額，不得超過針對最嚴重違法行為所定之罰鍰金額。

5. 科處罰鍰之程序

依 GDPR 第 83 條第 8 項，主管機關依該條科處罰鍰時，須依歐盟法和會員國法律，採行適當程序保障，包括有效之司法救濟及正當程序。

（二）法規立法理由

GDPR 前言第 148 點及第 150 點係關於行政罰鍰之說明。

第 148 點指出，行政罰鍰乃「強化 GDPR 執行」之措施。然而，若個案中違法行為尚屬輕微，或罰鍰可能對自然人造成過重負擔，得以告誡代替罰鍰。行政罰鍰之科處，應遵循正當法律程序。

第 150 點指出，GDPR 應規定罰鍰金額之上限，由主管機關審酌個案事實決定罰鍰之具體金額。若罰鍰對象為事業，應與歐盟運作條約（Treaty on the Functioning of the European Union, TFEU）第 101 條與第 102 條所稱之「事業」相一致；若非屬事業，則計算罰鍰金額時，應審酌該罰鍰對象所處會員國之收入水準，以及該對象自身之經濟狀況。

（三）實務運作標準

GDPR 生效前，個資保護指令（Directive 95/46/EC⁵）時代之第 29 條個資保護工作小組（Article 29 Data Protection Working Party, WP29）於 2017 年針對 GDPR 行政罰鍰問題發布指引（以下稱 WP29 指引）⁶，詳細分析第 83 條第 2 項所列各款事由應如何適用。GDPR 於 2018 年生效後，歐洲個人資料保護委員會（EDPB）取代 WP29，成為歐盟層級 GDPR 解釋機關。EDPB 已採認 WP29 指引。2022 年 5 月，EDPB 為提升會員國主管機關科處裁罰作業之一致性，發布《依 GDPR 計算

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.

⁶ WP29, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253) (3 October 2017).

行政罰鍰之指引 04/2022》（以下稱 EDPB 指引），針對 GDPR 行政罰鍰之計算提出統一之方法與步驟。EDPB 指引與 WP29 指引彼此補充，共同適用。下文將以 EDPB 指引為重點，分析依 GDPR 科處行政罰鍰之步驟及考量事由。

1. 識別罰鍰所涉之違法行為

計算行政罰鍰之前提，係正確識別該罰鍰所涉之行為。依所涉行為是否屬於「一行為」、行政罰鍰之上限、違反法規之判斷等，將須遵循不同規則。

EDPB 認為，在計算行政罰鍰前，首先應評估裁罰對象之行為數量，並分析其競合樣態，判斷 GDPR 第 83 條第 3 項之適用性。此階段分為三個步驟，即：

- 判斷裁罰對象是否構成「一行為」或「數行為」；
- 若構成一行為，判斷其是否違反數項不同規範；
- 若違反數項不同規範，該等規範間是否為法條競合，或想像競合。

(1) 「一行為」之判斷

EDPB 認為，裁罰對象是否構成「一行為」，應個案判斷。若「一組運用作業」屬行為人基於同一決意（unitary will）所為，且具備背景（特別是所涉個資當事人、目的與性質之同一性）及時空之密接性，則屬「一行為」，即 GDPR 第 83 條第 3 項所稱之「彼此『關聯』之一組運用作業」。運用作業間之「關聯性」應依個案情形嚴格認定。EDPB 並舉例說明：

- 若一資料中介決定執行下列個資運用活動：在不具備法律依據之背景下，自第三方取得消費者訂單紀錄資料，利用該資料分析及預測消費者之行為模式，不將該等蒐集與分析作成紀錄，不向消費者踐行告知，且不應消費者對此提出之任何權利行使請求。則該個資運用活動屬基於同一決意所為之一行為，其所包含之各項個資運用作業間具備「關聯性」。

若主管機關經上述分析，認定裁罰對象屬「一行為」，且該行為僅違反一項規範，則應適用該規範之裁罰上限；但若該行為違反數項規範，則應視該等規範間的關係，判斷是否為「法條競合」或「想像競合」。若裁罰對象屬「數行為」，則依 GDPR 第 83 條第 3 項之反面解釋（argumentum e contrario），可就違反規範分別科處罰鍰，且其總額可超過針對最嚴重違法行為所定之罰鍰金額。

(2) 法條競合

若一行為同時違反數項規範，但該等規範在適用上存在彼此排除或吸收關係（通常是因為其規範目的相一致），則屬法條競合（concurrency of offences）。此時，應依特別法優先原則（principle of specialty）、補充原則（principle of subsidiarity）、吸收原則（principle of consumption）等原則，適用其中一規範，成立對該規範之違法行為，並適用該規範之裁罰上限。

針對特別法優先原則，EDPB 指出，該原則僅適用於數規範在個案中之規範目的相一致之情形。若數規範之規範目的不完全相同，則

非屬法條競合，主管機關得依該等數規範，同時科處多項罰鍰。例如，GDPR 第 5 條規定個資運用之基本原則，而同法之其他條文可能係某一基本原則之具體規範，但未充分呈現該原則之全部內涵。此時，該條文與第 5 條即非法條競合關係。

(3) 想像競合

若一行為同時違反數項規範，但該等規範在適用上並無彼此排除或吸收關係（通常是因為其規範目的彼此不同），則屬想像競合（ideal concurrence），此時將有 GDPR 第 83 條第 3 項之適用，罰鍰總額不得超過針對最嚴重違法行為所定之罰鍰金額。EDPB 認為，第 83 條第 3 項之「罰鍰總額」意味著主管機關應在計算罰鍰金額時，將各項規範之違反皆納入考量；而「針對最嚴重違法行為所定之罰鍰金額」，係指第 83 條第 4 項至第 6 項針對該行為所規定之罰鍰金額上限。因此，此時主管機關仍應明確宣告該行為同時違反多項規範，並在計算最終罰鍰金額時，考量對各項規範之違反情事。

EDPB 並指出，若在時空密接之背景下，反覆實施違反同一規範之多項個資運用作業，亦應有想像競合規範之適用。例如，若控管者在同一天內，違反 GDPR 第 6 條第 1 項，以連續行為，分批向不同個資當事人統一寄發 E-mail 廣告信，則屬於一行為。此時，該行為僅違反同一規範，並不在第 83 條第 3 項文義之範圍內。然基於平等原則之考量，應準用（*mutatis mutandis*）第 83 條第 3 項之規定。

2. 確定罰鍰之計算起點

EDPB 認為，行政罰鍰之計算，應以共同方法確定計算起點。對此，EDPB 列出三項考量要素，即：

- GDPR 第 83 條第 4 項至第 6 項對違法行為之分類；
- 依 GDPR 第 83 條第 2 項評估之違法行為嚴重性；
- 裁罰對象事業之年營業額。

(1) GDPR 第 83 條第 4 項至第 6 項對違法行為之分類

EDPB 認為，GDPR 第 83 條第 4 項所列行為之裁罰上限為 1000 萬歐元（或年營業額之 2%），而第 5 項和第 6 項所列行為之裁罰上限為 2000 萬歐元（或年營業額之 4%），係立法者對相關違法行為嚴重程度之初步分類。

(2) 依違法行為嚴重性，確定計算起點之金額範圍

EDPB 將違法行為之嚴重性劃分為低、中、高三個類別，並據此劃定罰鍰金額之起算級距。GDPR 第 83 條第 2 項第 a 款所列「違法行為之性質、重大性及持續期間」、第 b 款所列「違法行為之故意或過失性質」，以及第 g 款所列「違法行為所涉之個資類別」，係確定違法行為嚴重性的考量要素。主管機關應綜合考量前述要素，認定違法行為嚴重性程度，進而搭配違法行為之法定罰鍰金額上限，依級距確定罰鍰金額計算起點之範圍。

(a) 違法行為嚴重性之評估

(i) 違法行為之性質、重大性及持續期間

違法行為之性質方面，主管機關應評估遭違反之規範所欲保護之法益，以及該規範在個資保護法制框架內的作用。此外，主管機關亦可考量該違法行為對該規範保護目的之妨礙程度。

違法行為之重大性方面，主管機關應依據個案之事實，綜合考量以下要素：

- 所涉運用之性質，包括運用之背景（商業活動、非營利活動、政黨活動等）及運用之一切特徵。若該運用在性質上具有高風險（例如涉及自然人人格特質之分析），或個資當事人與控管者間顯有權力不對等（例如當事人為員工或病患），或個資當事人為弱勢族群（例如兒童），則主管機關可對本要素賦予較高權重。
- 所涉運用之範圍，包括地域範圍（地區性、國家性或跨國性），以及運用之實際程度（依控管者對運用所投入之資源判斷）。運用之範圍越廣，主管機關遏止違法行為之難度越高，可對本要素賦予之權重亦越高。
- 所涉運用之目的。運用之目的越接近控管者之核心活動，主管機關可對本要素賦予之權重越高。此外，縱使運用活動與控管者之核心活動尚有距離，亦可能對評估有重大影響（例如，運用作業涉及員工個資處理，但違反情事嚴重損害員工之人性尊嚴）。
- 所涉個資當事人之數目，包括實際影響及潛在影響之當事人數目，以及受影響之當事人數目在相關當事人總數（例如相關市民、消費者、員工等）中所占比例。

受影響之個資當事人數目越高，主管機關可對本要素賦予之權重越高。

- 所涉損害之程度，以及違法行為對當事人權利與自由之影響。損害包括人身、財產及非財產方面的實際損害與潛在損害。但主管機關對損害程度之評估，應以正確判斷違法行為重大性為限，無須達到司法活動中損害判斷之程度。

違法行為之持續期間方面，通常而言，違法行為持續期間越長，主管機關可對本要素賦予之權重越高。在不違反會員國法之前提下，主管機關亦可考量 GDPR 生效前之違法行為。

關於此項考量要素，WP29 亦指出，依 GDPR 前言第 148 點之意旨，若個案中違法行為尚屬輕微，未對相關當事人之權利造成重大風險，亦未影響所涉個資保護義務之本質，則主管機關「得」（但並非「應」）決定以「告誡」代替罰鍰⁷。

(ii) 違法行為之故意或過失性質

EDPB 援用 WP29 之指引，認為通常而言，「故意」係指對違法行為有認識（knowledge）及決意（wilfulness）。例如，若違法行為係由最高管理層明確授權，或違背個資保護長之建議或無視政策實施違法行為等，則可認為存在故意。

「非故意」則指對違法行為並無認識或決意，但違反注意義務實施違法行為。忽視既有政策、人為疏失、疏未檢查所揭露資

⁷ WP29, Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679 (WP 253) (3 October 2017), 9.

訊中所含個資、疏未及時安裝技術更新、未訂定政策（而非單純未適用政策）等，可認為存在過失。

故意與過失之判斷，應將個案中行為之客觀要素納入判斷。通常而言，故意違反表現出對法規範之蔑視，其情節較過失更重。若涉及故意違反，主管機關得對本要素賦予更高權重。依個案事實，過失之程度亦可作為重點考量要素。過失至多為中性情節。

(iii) 違法行為所涉個資類別

GDPR 已明文規定某些類別之個資應受特別保護。此類個資至少應包括第 9 條規定之特種個資、第 10 條規定之犯罪前科資料，以及一經散布即可對當事人造成立即性損害或精神痛苦之個資，例如位置資料、私人通訊資料、國民身分證號，或財務資料（例如交易記錄或信用卡號）等。

通常而言，所涉此類資料之數量越多、資料之敏感性越高，主管機關得對本要素賦予之權重越高。此外，運用所涉單一當事人之資料量，也是考量要素之一。

(b) 依嚴重性確定罰鍰金額計算起點之金額範圍

主管機關應綜合考量違法行為性質、重大性、持續期間、故意或過失性質、所涉個資類別等要素，認定違法行為具備低度、中等或高度嚴重性，並配合該行為之法定罰鍰金額上限，確定罰鍰金額計算起點之範圍：

- 若違法行為具備低度嚴重性，則罰鍰金額計算起點之範圍為法定罰鍰金額上限的 0% 至 10%；

- 若違法行為具備中等嚴重性，則罰鍰金額計算起點之範圍為法定罰鍰金額上限的 10%至 20%；
- 若違法行為具備高度嚴重性，則罰鍰金額計算起點之範圍為法定罰鍰金額上限的 20%至 100%。

(3) 依裁罰對象事業之年營業額，衡酌計算起點之具體金額

主管機關得依裁罰對象事業之年營業額，調整計算起點之金額範圍，並衡酌確定計算起點之具體金額：

(a) 針對中小企業之調整

若裁罰對象為中小企業（micro, small and medium-sized enterprises, SME），主管機關針對依嚴重性確定之計算起點金額範圍，得依下列原則予以調整。主管機關應依調整後的金額範圍，確定罰鍰計算起點之具體金額：

- 若事業之年營業額未達 200 萬歐元（微型企業），則其裁罰計算起點之金額範圍，至多可調降至原本範圍之 0.2%；
- 若事業之年營業額未達 1000 萬歐元（小型企業），則其裁罰計算起點之金額範圍，至多可調降至原本範圍之 0.4%；
- 若事業之年營業額未達 5000 萬歐元（中型企業），則其裁罰計算起點之金額範圍，至多可調降至原本範圍之 2%。

(b) 針對一般事業之調整

EDPB 考量一般事業營業額之差異，亦劃定計算起點預定金額之調整方式：

- 若事業之年營業額超過 5000 萬歐元但未超 1 億歐元，則其裁罰計算起點之金額範圍，至多可調降至原本範圍之 10%；
- 若事業之年營業額超過 1 億歐元但未超 2.5 億歐元，則其裁罰計算起點之金額範圍，至多可調降至原本範圍之 20%；
- 若事業之年營業額超過 2.5 億歐元，則其裁罰計算起點之金額範圍，至多可調降至原本範圍之 50%。

(c) 確定計算起點之例示

- (i) 一家年營業額達 80 億歐元的連鎖超市違反 GDPR 第 12 條。主管機關經評估後，認為違法行為嚴重性為低度。主管機關依下列步驟確定罰鍰金額計算起點：
- 該超市違反 GDPR 第 12 條，屬第 83 條第 5 項所列違法行為，因該超市年營業額達 80 億歐元，該違法行為之法定罰鍰金額上限為 3.2 億歐元。
 - 因該超市違法行為具備低度嚴重性，故罰鍰金額計算起點之範圍為法定罰鍰金額上限的 0%至 10%，即 0 至 3200 萬歐元。
 - 因該超市年營業額達 80 億歐元，故主管機關得衡酌違反情形，將其裁罰起點之金額範圍，至多降至依嚴重性所確定金額範圍之 50%。

- 主管機關綜合考量該超市違法行為之嚴重性及其相對較高之年營業額，認為 2500 萬歐元具備有效性、合比例性與嚇阻性，係適當之罰鍰金額計算起點。
 - 主管機關進而依 2500 萬歐元為起點，在 2500 萬至 3.2 億歐元範圍內，進一步計算最終裁罰金額。
- (ii) 一家年營業額達 50 萬歐元的新創企業違反 GDPR 第 9 條和第 5 條第 1 項，將客戶之特種個資販售予資料中介作分析用途。主管機關經評估後，認為違法行為嚴重性為高度。主管機關依下列步驟確定罰鍰金額計算起點：
- 該企業違反 GDPR 第 9 條和第 5 條第 1 項，屬第 83 條第 5 項所列違法行為，因該企業年營業額達 50 萬歐元，該違法行為之法定罰鍰金額上限為 2000 萬歐元。
 - 因該企業違法行為具備高度嚴重性，故罰鍰金額計算起點之範圍為法定罰鍰金額上限的 20%至 100%，即 400 萬至 2000 萬歐元。
 - 因該企業年營業額達 50 萬歐元，故主管機關得衡酌違反情形，將其裁罰起點之金額範圍，至多降至依嚴重性所確定金額範圍之 0.2%（即計算起點可低至 0.8 萬歐元）。
 - 主管機關綜合考量該企業違法行為之嚴重性及其相對較低之年營業額，認為 1.6 萬歐元具備有效性、合比例性與嚇阻性，係適當之罰鍰金額計算起點。
 - 主管機關進而依 1.6 萬歐元為起點，在 1.6 萬至 2000 萬歐元範圍內，進一步計算最終裁罰金額。

3. 評估罰鍰之加重或減輕情節

EDPB 指出，在確定罰鍰金額計算起點後，主管機關應繼續衡酌 GDPR 第 83 條第 2 項所列之其他加重或減輕情節。而第 83 條第 2 項第 a 款所列「違法行為之性質、重大性及持續期間」、第 b 款所列「違法行為之故意或過失性質」，以及第 g 款所列「違法行為所涉之個資類別」，因在「確定罰鍰金額計算起點」步驟已考量過，本步驟不得再予考量。

(1) 控管者或受託運用者為減輕個資當事人損害而採取之措施

依 GDPR 第 83 條第 2 項第 c 款，「控管者或受託運用者為減輕個資當事人損害而採取之措施」係評估罰鍰金額之考量要素之一。

EDPB 認為，控管者及受託運用者本就有義務採行技術性和組織性安全維護措施，降低其個資運用活動對個資當事人權益的侵害。如發生違法行為，控管者或受託運用者應盡其所能採取措施，降低違法行為對個資當事人之不利影響。

降低當事人損害的措施可作為減輕情節，降低罰鍰金額。若控管者或受託運用者在知悉違反情事後、主管機關開始調查前，即已主動採行因應措施，則更可能構成減輕情節。

(2) 控管者或受託運用者之責任程度

依 GDPR 第 83 條第 2 項第 d 款，「控管者或受託運用者之責任程度」係評估罰鍰金額之考量要素之一。

EDPB 援引 WP29 之指引，認為控管者或受託運用者的責任程度與其採取的個資保護措施密切相關，特別是 GDPR 第 25 條規定之資料保護「設計」與「預設」措施，以及第 32 條規定之安全維護措施。概言之，主管機關須評估，「考量個資運用之性質、目的或規模，從 GDPR 所定義務角度觀之，控管者是否『該做的都做到了』」。

此時，主管機關須評估控管者採取保護措施後，對個資當事人權利與自由之剩餘風險、所採取措施的穩健性（robustness）、所涉個資在未採取技術保護措施時的識別性等。

EDPB 並指出，控管者或受託運用者之責任程度可能是加重或中性情節。僅有控管者或受託運用者所採取之措施遠優於法規要求水準之例外情形下，責任程度才可能作為裁罰減輕情節。

(3) 控管者或受託運用者此前之違反情事

依 GDPR 第 83 條第 2 項第 e 款，「控管者或受託運用者此前之違反情事」係評估罰鍰金額之考量要素之一。EDPB 認為，此前違反情事之時間、標的等，皆為相關要素。

時間方面，若此前違反情事之發生時間越久遠，對當前裁罰之重要性越低。但另一方面，此前違法行為可能用以判斷控管者或受託運用者之過去表現（track record）。對 GDPR 之違法行為，重要性高於對個資保護指令（Directive 95/46/EC）所對應國內法之違反，後者能否納入考量，應以主管機關所處國家之國內法為準。

標的方面，無論前後違法行為之標的是否相同，皆應納入考量，但標的相同之違法行為，對當前裁罰之重要性較高。此外，若前後違

法行為雖標的不同，但違反方式相同（例如，皆涉及違反 DPO 之建議），則也應予以重視。

此前違法行為可作為計算罰鍰之加重情節。然而，若此前並無違反情事，亦不得作為減輕情節，蓋遵循行為應屬常態。

(4) 控管者或受託運用者為糾正違法行為、減輕不利影響而與主管機關之配合程度

依 GDPR 第 83 條第 2 項第 f 款，「控管者或受託運用者為糾正違法行為、減輕不利影響而與主管機關之配合程度」係評估罰鍰金額之考量要素之一。

EDPB 認為，依 GDPR 第 31 條，控管者或受託運用者本即負有配合主管機關之義務，且如違反第 31 條，可能依第 83 條第 4 項第 a 款遭受裁罰。因此，第 31 條意義上之配合義務應屬中性情節，而非減輕情節。

然而，若因配合主管機關，有效減輕或避免了本可能發生之當事人權利侵害後果，則可視為減輕情節。

(5) 主管機關知悉違法行為之方式，特別是控管者或受託運用者之通報狀況

依 GDPR 第 83 條第 2 項第 h 款，「主管機關知悉違法行為之方式」係評估罰鍰金額之考量要素之一。

EDPB 認為，尤其應考量在主管機關尚未知悉時，控管者或受託運用者是否——以及如何——主動向主管機關通報其違反情事。若主管機關係透過申訴、調查等獲知違反情事，原則應視為中性情節。若控管

者或受託運用者在主管機關知悉前主動通報，則可視為減輕情節。但若控管者本就負有通報義務（例如依 GDPR 第 33 條通報個資侵害事故），則主動通報僅可視作中性情節。

(6) 若主管機關前曾就同一標的科處糾正措施，控管者或受託運用者對該措施之遵循狀況

依 GDPR 第 83 條第 2 項第 i 款，「若主管機關前曾就同一標的科處糾正措施，控管者或受託運用者對該措施之遵循狀況」係評估罰鍰金額之考量要素之一。相較於第 e 款，本款僅涉及主管機關此前就同一標的，向同一控管者或受託運用者科處之糾正措施。

EDPB 認為，由於控管者或受託運用者本就有義務遵循主管機關之命令，因此落實糾正措施本身並不足以構成減輕情節。僅有當所採取之糾正措施超越主管機關之要求時，方可認其屬減輕情節。此外，若控管者或受託運用者未遵循此前科處之糾正措施，則可作為裁罰之加重情節，或依據 GDPR 第 83 條第 5 項第 e 款或第 83 條第 6 項另行處罰。

(7) 對 GDPR 第 40 條行為守則或第 42 條認證機制之遵循狀況

依 GDPR 第 83 條第 2 項第 j 款，「對 GDPR 第 40 條行為守則或第 42 條認證機制之遵循狀況」係評估罰鍰金額之考量要素之一。

EDPB 援引 WP29 之指引，認為某些情形下，遵循行為守則或認證機制可作為減輕情節。另一方面，若控管者或受託運用者未能遵循行為守則或認證機制，且該等情事與當前裁罰直接相關，則主管機關得將之作為加重情節。

(8) 其他加重或減輕情節

依 GDPR 第 83 條第 2 項第 k 款，主管機關於評估罰鍰金額時，得考量其他加重或減輕情節，例如因違法行為直接或間接所獲利益、所避免之損失等。

EDPB 認為，此款開放性規定係個案公平原則之體現。主管機關於適用本款時，應納入該控管者或受託運用者所處經濟社會背景之各項要素，包括法律背景與市場背景。例如，如可證明控管者或受託運用者因違法行為而獲得經濟利益，則可作為加重要素。此外，經濟社會背景之劇烈變化（例如出現嚴重疫情，以致顯著改變個資運用方式），也可納入考量。

4. 確認法定罰鍰金額上限

GDPR 並未針對特定違法行為規定具體罰鍰金額，而是於第 83 條第 4 項、第 5 項與第 6 項，規定違法行為之罰鍰金額上限。主管機關所定之罰鍰金額，不得超出法定上限。EDPB 指出，罰鍰上限係針對單一違法行為所設，主管機關在適用裁罰上限時，須考量是否有第 83 條第 3 項規定情形。

(1) 固定上限與浮動上限

EDPB 指出，依 GDPR 第 83 條，罰鍰金額原則採固定上限，即該條第 4 項所列違法行為之上限為 1000 萬歐元，而第 5 項和第 6 項所列行為之裁罰上限為 2000 萬歐元。然而，若違反者為事業，且其前一年度全球營業額達 5 億歐元，則適用浮動上限，即該條第 4 項所

列違法行為之上限為年營業額之 2%，而第 5 項和第 6 項所列行為之上限為年營業額之 4%。

EDPB 併舉例指出，若違法行為人為公務機關或機構，則不屬於「事業」，不適用浮動上限。此時，原則應適用固定上限處以罰鍰，但該公務機關所處會員國得依 GDPR 第 83 條第 7 項，就可否及如何針對公務機關或機構科處罰鍰另定規範。

(2) 事業年營業額之計算

GDPR 立法理由第 150 點指出，計算對事業之行政罰鍰時，「事業」之含義，應與歐盟運作條約（Treaty on the Functioning of the European Union, TFEU）第 101 條與第 102 條所稱之「事業」相一致。EDPB 指出，依第 83 條計算罰鍰時之「事業」之概念，與 GDPR 第 4 條第 18 款所稱「企業（enterprise）」之概念應相區分。後者之概念主要見於 GDPR 第 5 章中，關於「企業團體（group of enterprise）」之規範。

(a) 事業之定義

依歐盟法院（Court of Justice of the European Union, CJEU）之見解，「事業」可包括從事經濟活動之各類實體，無論其法律地位或資金來源。因此，「事業」係一經濟意義的單位，而非法律意義上的單位，同一集團內的多家公司可能構成同一經濟單位，進而屬於同一事業。

TFEU 第 101 條及第 102 條所稱之事業，係指單一經濟單位（single economic unit, SEU），且該 SEU 可能由多個自然人或法人組成。多個實體是否構成同一 SEU，主要取決於各該實體是否有獨立決策權，

或由其中一實體（母公司）對其他實體施加「決定性影響」（decisive influence）。而「決定性影響」之判斷，須依母公司與子公司間經濟上、法律上及組織上之連結而定（例如，母公司對子公司之參與狀況、人員或組織關聯性、指示狀況、母子公司間契約狀況等）。

若子公司違反 GDPR，則主管機關依第 83 條科處罰鍰時，須依下列方式判斷其與母公司是否構成同一 SEU：

- 若母公司持有子公司 100%或接近 100%之股權，則推定該母公司對子公司施加決定性影響（即「Akzo 推定⁸」），母公司與子公司構成同一 SEU。此時之持股之計算，不以直接持有為限，亦包括透過其他子公司間接持有之股權。然而，Akzo 推定得於個案中舉證推翻。母子公司須提出經濟上、法律上及組織上連結之相關證據，證明母公司雖持有子公司 100%或接近 100%之股權，子公司仍係獨立運作。
- 另一方面，若母公司並未直接或間接持有子公司 100%或接近 100%之股權，則須由主管機關證明母子公司構成同一 SEU。此時，主管機關不僅須證明母公司「能夠」對子公司施加決定性影響，還必須證明母公司確實已對子公司施加該決定性影響，以至於其可隨時介入子公司之

⁸ CJEU, Case C-97/08 P, Akzo Nobel NV and Others v Commission of the European Communities, paras 60~63. 歐盟法院於該案中認為，若母公司持有子公司 100%之股權，則母公司能夠對子公司之行為施加決定性影響（exercise a decisive influence），且可「推定」母公司對子公司之行為實際施加決定性影響。此時，競爭法主管機關歐盟執委會僅須證明母公司對子公司 100%持股，即可要求母公司對子公司之行為負連帶責任。母公司須自行舉證其未實際施加決定性影響，推翻該推定，方可免責。

決策與行為。至於母公司對子公司指示之性質或類型，則在所不問。

若子公司違反 GDPR，則主管機關之裁罰決定，應以子公司為裁罰對象。然若該子公司與其母公司、其他實體構成同一 SEU，則主管機關得在針對子公司之裁罰決定中，命令同一 SEU 內之其他實體對罰鍰負連帶責任。

EDPB 並援用歐盟法院之見解指出，GDPR 第 83 條第 4 項至第 6 項之適用，遵循「企業直接責任」（direct corporate liability）原則。亦即，經授權代表事業之自然人之故意或過失行為，視為該事業自身之故意或過失行為。僅有該自然人係為自己或他人之目的從事個資運用，從而成為該運用之控管者時，才可排除企業直接責任原則。此外，企業直接責任下，代表事業之自然人不以具備特定職位（例如總經理）為限；且主管機關及會員國法院無須具體列明代表企業為違法行為之自然人。

(b) 事業年營業額之計算方式

EDPB 指出，若控管者或受託運用者屬於某一事業（之一部分），則主管機關得以該事業總體之年營業額作為確定罰鍰金額上限之基準，以利確保裁罰之有效性、合比例性與嚇阻性。

年營業額之範圍方面，GDPR 第 83 條所稱之年營業額，係指「淨營業額」（net turnover），即銷售或出租產品或服務之總收入，扣除折扣額和營業稅（value-added tax, VAT）後之淨額。因此，營業額不包括企業非因業務活動而取得的收入（例如製造業者出售固定資產或

出租閒置辦公空間之收入)。淨營業額之計算，應以該事業會計帳簿中損益表「淨營業額」一欄所載金額為準。若事業依法須準備合併報表，則可依據合併報表確定該事業之總體營業額。

年營業額計算之時間基準方面。EDPB 參酌歐盟法院關於競爭案件年營業額之時間基準，認為 GDPR 第 83 條所稱之「上一年度」，應以「主管機關作出裁罰決定時」為基準，而非「違法行為時」或「法院判決時」。若該裁罰案件具跨境性質，須經 GDPR 第 7 章之一致性機制，即以主管機關作出「最終裁罰決定時」為基準，而非以「裁罰決定草案」作出時為準。此時，若主責主管機關提出裁罰決定草案時已是當年年底，則最終裁罰決定很可能無法於同一年度內作出。此時，主責主管機關在裁罰決定草案中，應使用當時可得之最新財務報表資料計算罰鍰金額；而在作出最終決定前，應重新計算罰鍰金額。

5. 評估裁罰金額之妥適性

主管機關應評估其擬科處之罰鍰金額，是否符合 GDPR 第 83 條第 1 項「有效性」、「合比例性」與「嚇阻性」要求。

EDPB 認為，「有效性」要求該裁罰足以回復法秩序之遵循狀態，和（或）足以懲罰違法行為。此外，依據 GDPR 立法理由第 148 點，「為強化本規則之執行，應對違法行為科處行政罰鍰」。因此，主管機關應確保其罰鍰滿足該等目標。

基於「合比例性」要求，主管機關之裁罰須與違法行為之嚴重性、以及行為人之規模整體相當，且不得超出實現 GDPR 規範目的（亦即，遵循自然人個資保護及個資自由流動之相關規範）之必要範圍。在特殊例外情形下，主管機關得考量過苛原則（principle of inability to

pay)，酌減罰鍰金額。然而，參酌歐盟執委會關於行政罰款之相關指引⁹，須存在客觀證據，表明該罰鍰將不可逆地損害該事業之經濟可行性（economic viability）時，方可為此等酌減：

- 經濟可行性：該事業須提供詳盡之財務資料（至少過去五年之財務資料，以及當年度及未來兩年之財務預估），供主管機關評估清償能力、流動性與獲利能力之關鍵指標。依歐盟法院之見解，事業當前或裁罰後財務狀況不佳之單純事實，尚不足以適用過苛原則，否則「無異於使最不適應市場環境之事業獲取不當之競爭優勢」。罰鍰是否過苛之判斷，亦考量重整計畫之可行性及其實施狀況、與銀行等外部財務伙伴之關係等。
- 價值減損之證明：若裁罰將損及事業之經濟可行性，導致其資產喪失全部或大部分價值時，方可適用過苛原則酌減裁罰。裁罰與價值減損間須具有因果關係，且破產並不必然意味著價值減損。事業應證明其可能退出市場，且其財產將大幅折價出售，而無法（自行或由他人）繼續營運。因此，主管機關應要求該事業證明，並無跡象表明其自身或資產可能被他人收購後繼續營運。
- 特定經濟社會背景：主管機關得考量該行業所處之特定經濟或社會背景，例如行業性景氣危機、區域性高失業率等。此外，亦可考量支付罰鍰對上下游行業可能導致的失業或衰退影響。

⁹ EU Commission, Commission Guidelines on the method of setting fines imposed pursuant to Article 23(2)(a) of Regulation No 1/2003 (2006/C 210/02).

基於「嚇阻性」要求，裁罰須確有嚇阻效果，包括一般性嚇阻（防範他人實施相同違法行為）與特別性嚇阻（防範該行為人再次實施相同違法行為）。裁罰之嚇阻性，不僅取決於裁罰之性質和金額，亦包括科處裁罰之可能性。嚇阻性要求行為人害怕將因此遭受裁罰；在此方面，嚇阻性與有效性內涵有所重疊。若主管機關認為裁罰之嚇阻性不足，得酌增罰鍰金額。

6. 其他說明

EDPB 指出，其指引僅提供計算行政罰鍰之一般性方法，不應將該方法誤解為計算罰鍰之固定公式。實際科處之罰鍰金額，皆須由主管機關之人員綜合評估所有情節後具體認定，且必須在個案中具備有效性、合比例性與嚇阻性。

主管機關得衡酌是否針對特定違反情事預定其裁罰金額，但其預定金額之適用，並不影響該主管機關遵循依 GDPR 第 7 章一致性程序之義務。此外，主管機關宜將其預定金額事先通知其他會員國之主管機關。

（四）案例

2021 年，全球即時通訊軟體業者 WhatsApp，被愛爾蘭個資保護委員會（Data Protection Commission, DPC）以違反 GDPR 為由，裁罰 2.25 億歐元¹⁰（以下稱 WhatsApp 案）。該案裁罰決定作成過程中，

¹⁰ Irish DPC, Data Protection Commission announces decision in WhatsApp inquiry (02 September 2021), <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry>; Irish DPC, Decision in the matter of WhatsApp Ireland

罰鍰金額為爭議焦點之一。EDPB 針對該案作出有拘束力之決定（Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR，以下稱第 1/2021 號決定）¹¹，並於該決定中，就 GDPR 第 83 條規範作詳盡分析。前述 EDPB 指引之部分內容，即係基於第 1/2021 號決定之分析發展而來。

1. 事實背景

愛爾蘭 DPC 於 2018 年 12 月依職權對 WhatsApp 愛爾蘭子公司 WhatsApp Ireland Limited,（以下稱 WhatsApp IE）之 GDPR 遵循狀況進行調查，並於 2020 年 12 月作出裁罰決定草案。愛爾蘭 DPC 於裁罰決定草案中認為 WhatsApp IE 違反 GDPR 第 12 條、第 13 條和第 14 條，預估行政罰鍰金額將介於 3000 萬至 5000 萬歐元間¹²。

因 WhatsApp 在歐盟的服務範圍涵蓋多個會員國，構成 GDPR 第 4 條第 23 款之「跨境運用」個人資料，愛爾蘭對該案作出正式裁罰決定前，首先依 GDPR 第 60 條，將其裁罰決定草案送交其他會員國之個資保護主管機關。法國、德國、荷蘭、義大利、波蘭、葡萄牙、匈牙利等多個國家的個資保護主管機關分別針對裁罰決定草案提出異議。在行政罰鍰部分，其他會員國主管機關針對預估罰鍰金額之計算

Limited made pursuant to Section 111 of the Data Protection Act 2018 (hereinafter, “Irish DPC Decision”), https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf.

¹¹ EDPB, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR (28 July 2021) (hereinafter, “EDPB Binding decision”).

¹² EDPB Binding decision, para 345.

基礎、對第 83 條第 3 項競合規範之解釋、對第 83 條第 1 項及第 2 項之解釋，其他會員國主管機關皆提出不同意見¹³。

為解決會員國間關於該案裁罰決定之爭議，EDPB 於 2021 年 7 月，作出第 1/2021 號決定，經分析 GDPR 第 83 條於該案之適用後，要求愛爾蘭 DPC 重新評估行政罰鍰之計算基礎、合比例性等，確定更高之罰鍰金額。愛爾蘭 DPC 因受 EDOB 該決定拘束，而於 2021 年 8 月 20 日作出正式裁罰決定，對 WhatsApp IE 科處 2.25 億元罰鍰。

WhatsApp IE 不服裁罰決定，除向愛爾蘭國內法院針對愛爾蘭 DPC 之正式裁罰決定起訴外，並於 2021 年 11 月 1 日向歐盟法院起訴，請求歐盟法院撤銷 EDPB 第 1/2021 號決定¹⁴。歐盟法院於 2022 年 12 月 7 日以第 1/2021 號決定未顯著變動（bring about a distinct change）WhatsApp 之法律地位，而以當事人不適格為由，裁定駁回其起訴¹⁵，然認為愛爾蘭國內法院得於審理愛爾蘭 DPC 正式裁罰決定之訴訟時，一併審查第 1/2021 號決定，並在認為第 1/2021 號決定有違法之虞時，請求歐盟法院對該決定予以審查。

2. 罰鍰之計算基礎：前一會計年度年營業額之確定

(1) 裁罰草案之見解

¹³ EDPB Binding decision, para 10.

¹⁴ WhatsApp Ireland v EDPB (Case T-709/21), Action brought on 1 November 2021,
<https://curia.europa.eu/juris/document/document.jsf?text=&docid=251744&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=2953747>.

¹⁵ WhatsApp Ireland v EDPB (Case T-709/21), Order of The General Court, 7 December 2022,
<https://curia.europa.eu/juris/document/document.jsf?text=&docid=268419&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2953747>.

愛爾蘭 DPC 於其裁罰決定草案中認定，WhatsApp IE 與其母公司 Facebook, Inc. 構成同一事業，並將兩家公司 2019 年度年營業額之加總金額作為計算罰鍰金額上限之基礎。

(2) 相關主管機關之異議

對於裁罰決定草案中上述見解，其他會員國主管機關提出之異議包括：

- (a) 罰鍰金額上限之計算，應以「整個 Facebook 集團」之年營業額加總為基礎（異議①）。
- (b) 應以 2020 年的年營業額為計算基礎（異議②）。
- (c) 確定具體罰鍰金額時，應將年營業額作為考量要素之一，以確保裁罰之嚇阻性與有效性（異議③）。

(3) 愛爾蘭 DPC 之回應

愛爾蘭 DPC 針對異議①與②，表示其將考量以「整個 Facebook 集團」之年營業額作為計算基礎，並將於作出正式裁罰決定時，改以 2020 年度之年營業額為基礎。但針對異議③，認為年營業額僅用於確定罰鍰金額之法定上限，並非確定具體罰鍰金額時之考量要素。

(4) EDPB 之分析

EDPB 對上述異議的分析如下：

(a) 事業之年營業額

EDPB 指出，依歐盟法院之見解，若母公司及其子公司構成單一事業（single undertaking），則縱使母公司未直接參與子公司之行為，

子公司之行為仍可歸屬於母公司。此時，母公司可能須負罰鍰責任。此外，若母公司與子公司構成單一事業，且該事業須對子公司之違法行為負責，則應以該事業內所有成員公司年營業額之總和，作為計算該事業經濟狀況之基礎。

因此，EDPB 要求愛爾蘭 DPC 修正其裁罰決定草案，將該單一事業內所有成員公司年營業額之總和，作為依 GDPR 第 83 條計算罰鍰之基礎。

(b) 年營業額之時點

EDPB 指出，在競爭法領域，歐盟法院認為，歐盟執委會作出裁罰時，應以裁罰當時前一年度之年營業額為計算基礎。GDPR 與競爭法皆是通過正式裁罰決定確定罰鍰金額，因此得參考歐盟法院之意見，以「正式裁罰決定作出時」為「前一年度」之計算時點。

然對於「跨境運用」個人資料之違法行為，GDPR 設有一站式 (one-stop-shop) 機制，主責主管機關 (lead supervisory authority, LSA) 須將裁罰決定草案分送相關主管機關 (concerned supervisory authority, CSA)。考量裁罰決定草案與正式決定間之時間間隔，EDPB 認為裁罰決定草案中，得暫以當時可得之最新財務資料為計算依據。

(c) 年營業額作為確定具體罰鍰金額之考量要素

年營業額可否作為確定具體罰鍰金額之考量要素，與 GDPR 第 83 條第 1 項裁罰之有效性、合比例性與嚇阻性密切相關，因此將與第 83 條第 1 項之其他異議一併分析。

3. GDPR 第 83 條第 3 項之解釋

(1) 裁罰草案之見解

愛爾蘭 DPC 於其裁罰決定草案中認為，WhatsApp IE 之行為，係以同一組運用作業，同時違反 GDPR 第 12 條、第 13 條和第 14 條。依據第 83 條第 3 項「行政罰鍰之總額，不得超過針對最嚴重違法行為所定之罰鍰金額」之規範，愛爾蘭 DPC 認為 WhatsApp IE 最嚴重的違法行為，係對 GDPR 第 14 條之違反。因此，裁罰決定草案擬僅針對該違反科處裁罰，且罰鍰金額不得超過針對違反第 14 條所定之最高金額。

(2) 相關主管機關之異議

對於裁罰決定草案中上述見解，其他會員國主管機關提出之異議包括：

- 愛爾蘭 DPC 對 GDPR 第 83 條第 3 項之解釋與立法者本意不符。愛爾蘭 DPC 對該項之解釋，將在事實上造成不處罰較輕違法行為之效果。因此，主管機關仍應明確認定處罰對象之行為同時違反各項條文。
- GDPR 第 83 條第 3 項規定，「行政罰鍰之『總額』（total amount），不得超過針對最嚴重違法行為所定之罰鍰金額」，由其文意可知，該項應適用於數罰鍰金額之「加總」。然依據愛爾蘭 DPC 對該項之解釋，若裁罰對象「同時違反多項規範」，其罰鍰金額將與「僅違反一項規範」相同，而對其他規範之違反，將無法納入罰鍰金額之考量中。
- GDPR 第 83 條第 3 項規定，「行政罰鍰之總額，不得超過針對最嚴重違法行為『所定之』（specified）罰鍰金

額」。此處「所定之」金額，應係 GDPR 針對最嚴重違法行為所規定的罰鍰金額的「抽象上限」。因此，若同時違反多項規範，應分別計算其罰鍰金額，但各項罰鍰金額之加總，不得超過 GDPR 針對最嚴重違法行為所規定的法定上限。

(3) 愛爾蘭 DPC 之回應

針對前述異議，愛爾蘭 DPC 認為，實務中各國主管機關對 GDPR 第 83 條第 3 項之解釋與適用並不一致，且其所採取之解釋，並未違反 GDPR 第 83 條第 3 項之文義與目的。主管機關應對違反的嚴重性進行個案判斷，而非以第 83 條第 4 項、第 5 項（關於罰鍰上限之規定）作為抽象劃分標準。若第 83 條第 3 項係關於複雜情形中法定罰鍰上限之規範，其在體系上應置於第 83 條第 4 項、第 5 項之後，而非之前。此外，無論主管機關如何適用第 83 條第 3 項，其皆須依第 83 條第 1 項，確保裁罰在個案中之有效性、合比例性與嚇阻性，包括調整罰鍰金額，以及依第 58 條第 2 項科處其他糾正措施。

(4) EDPB 之分析

EDPB 認為，上述異議的核心在於，當違反多項規範時，GDPR 第 83 條第 3 項之規範，將如何影響罰鍰金額之計算。

首先，第 83 條第 3 項僅適用於「一組運用作業」同時違反多項規範之情形。

其次，依據有效解釋原則（*effet utile principle*），對歐盟法之解釋應充分實現其效力。然愛爾蘭 DPC 對第 83 條第 3 項之解釋，若一

組運用作業同時違反多項規範，則罰鍰金額將與「僅違反一項規範（即最嚴重者）」相同，對其他規範之違反（無論違反多少項規範），將對罰鍰金額無影響。此一解釋不利於 GDPR 之全面執行與遵循，因此不符立法目的。

EDPB 認為，如一組運用同時違反數項規範，則可確定數項罰鍰，但各項罰鍰之加總金額，不得超過 GDPR 就最嚴重違法行為規定的罰鍰金額抽象上限，亦即第 83 條第 4 項至第 6 項規定之法定上限。此外，第 83 條第 3 項規定「行政罰鍰之『總額』」，亦表明計算罰鍰金額時，須考量對其他規範之違反。

EDPB 進而指出，如控管者的一組運用同時違反數項規範，則主管機關應明確認定該控管者同時違反所涉全部規範，並在計算罰鍰時，將各項違反皆納入考量範圍，但所科處的罰鍰金額，不得超過最嚴重違法行為依第 83 條第 4 項至第 6 項應適用之法定上限。

4. GDPR 第 83 條第 1 項與第 2 項之解釋

(1) 裁罰草案之見解

(a) 第 83 條第 2 項

愛爾蘭 DPC 於其裁罰決定草案中，分析第 83 條第 2 項所列各項事由。其中，第 a 款、第 b 款、第 d 款、第 k 款遭相關主管機關提出異議，該四款之分析如下：

首先，針對第 83 條第 2 項第 a 款之「違法行為之性質、重大性及持續期間」，愛爾蘭 DPC 認為該案涉及當事人知的權利，此一權利乃個資保護之基石；WhatsApp IE 在該案中嚴重違反 GDPR 第 14 條規範，完全未向「非用戶（non-user）」踐行告知；該違法行為自

GDPR 於 2018 年 5 月 25 日生效後，一直持續存在；該違法行為所涉個資運用程度不高（主要目的是為實現用戶之互聯），但涉及大量用戶及非用戶。

針對第 83 條第 2 項第 b 款之「違法行為之故意或過失性質」，愛爾蘭 DPC 認為 WhatsApp IE 之違法行為係出於過失，並將其作為加重事由。

針對第 83 條第 2 項第 d 款之「控管者或受託運用者之責任程度」，愛爾蘭 DPC 認為 WhatsApp IE 完全未向非用戶踐行告知，應屬加重事由。

針對第 83 條第 2 項第 k 款之「其他加重或減輕事由」，愛爾蘭 DPC 認為，其難以確定「提升透明性是否將對 WhatsApp 的用戶基數之持續增長造成不良影響」，因而將其視為中性事由。

(b) 第 83 條第 1 項

愛爾蘭 DPC 於其裁罰決定草案中認為，其擬科處之裁罰符合有效性、合比例性、嚇阻性要求，且從 WhatsApp 用戶規模、違法行為之影響、當事人權益保障、歐盟個資保護法制目的之角度，未超出落實遵循 GDPR 之必要範圍。愛爾蘭 DPC 並援用法國個資保護主管機關對 Google 的裁罰決定，認為由違反事實嚴重性角度觀察，兩案之罰鍰金額具相當性。

(2) 相關主管機關之異議

對於裁罰決定草案中上述見解，其他會員國主管機關提出之異議包括：

- 對於裁罰對象而言，裁罰決定草案之罰鍰金額幾乎不值一提（hardly noticeable），而無嚇阻效果，違反第 83 條第 1 項要求。
- 裁罰決定草案僅識別少數減輕事由，但認為 WhatsApp IE 存在重大違反情事，且影響大量當事人（3.26 億用戶及 1.25 億非用戶），所課罰鍰應接近法定上限方屬適當。
- WhatsApp IE 明知提升透明性可能阻礙其用戶基數的持續增長，係為了營利而未遵守 GDPR；且 2012 年荷蘭主管機關曾向 WhatsApp 指出向非用戶踐行告知之問題。因此，其違法行為應係出於故意，而非過失。

(3) 愛爾蘭 DPC 之回應

針對前述異議，愛爾蘭 DPC 認為，違法行為之性質方面，經濟收益並非評估故意或過失之考量因素。違法行為之嚴重性及對當事人權益之影響方面，WhatsApp IE 的違法行為對當事人權益之風險相對較小，集中表現於「非用戶註冊為用戶之當下」，在此範圍外，非用戶得行使之權利相當有限，因此，雖然違反較為嚴重，但當事人之影響不應高估。此外，行為人對罰鍰金額之敏感性（sensitivity to punishment）僅為德國法之原則，而非歐盟法規範，因此其無從適用該原則。

(4) EDPB 之分析

(a) 第 83 條第 2 項

EDPB 基本認同愛爾蘭 DPC 對 GDPR 第 83 條第 2 項所列各項事由之衡酌。

例如，違法行為之性質方面，EDPB 指出，違法行為之「故意」或「過失」性質，應依個案客觀事實判斷；歐盟法院見解，「過失」包括對潛在之違法行為有認識，但未依法律要求採取措施之情形；且「故意」包括「認識」與「決意」兩項不同要素。愛爾蘭 DPC 在該案中已查明之事實，不足以表明 WhatsApp 存在違反法律之決意，因此應屬過失。

此外，愛爾蘭 DPC 已充分評估違法行為之嚴重性、對當事人權益之影響、受影響之當事人數目、行為人責任程度等事由，認為 WhatsApp 對當事人之告知內容遠未達到 GDPR 要求水準，直接衝擊個人資料保護之基本權的核心領域，且涉及大量當事人，因此違反性質嚴重且具重大性；WhatsApp 對其違法行為，存在高度過失。愛爾蘭 DPC 雖認為該案中存在減輕事由（違法運用之個人資料僅限手機號碼），但認為該事由在整體考量中不應給予較高權重。相關主管機關之異議，或在個案中缺乏客觀證據，或已由愛爾蘭 DPC 作適當審酌。

(b) 第 83 條第 1 項

EDPB 指出，依愛爾蘭 DPC 之見解，GDPR 第 83 條第 2 項並未將年營業額列作考量事由之一，因此，裁罰對象的年營業額僅用以確定罰鍰金額法定上限，而與個案中罰鍰金額之計算無關，否則將違反法律明確性原則。然而，愛爾蘭 DPC 的見解並不適當。

首先，GDPR 第 83 條第 4 項至第 6 項將事業之「年營業額」作為確定罰鍰金額法定上限之基礎，其目的在於確保主管機關能夠對大

型事業科處有效、合比例且具嚇阻性之罰鍰。因此，事業之規模（以年營業額評量）應作為罰鍰金額之考量要素，以確保罰鍰之有效性、合比例性及嚇阻性。

雖然第 83 條第 2 項與第 3 項皆無「年營業額」之明文，然並不意味著年營業額「僅與」罰鍰金額法定上限有關。首先，在第 83 條第 1 項已要求罰鍰金額應有效、合比例且具嚇阻性之前提下，第 2 項與第 3 項應無須另行規定年營業額，蓋主管機關得於法定上限之範圍內，裁量行使其裁罰權，以實現裁罰之有效性、合比例性及嚇阻性。其次，若 GDPR 一方面導入「浮動上限」之規範，將事業之年營業額作為確定法定上限之基礎，另一方面於個案計算罰鍰金額時，卻禁止主管機關考量事業年營業額而調整罰鍰金額、落實罰鍰之有效性、合比例性及嚇阻性，則屬自相矛盾之解釋。此外，第 83 條第 2 項並非完全列舉應考量之全部事由，第 k 款之文義亦表明，主管機關得考慮未明文列舉之其他事由。

EDPB 強調，為確保有效性，罰鍰應與個案情節相當，這不僅包括與個案之違法行為相當，亦包括與實施違反之行為人相當（即符合其財務狀況）。此外，依歐盟法院之見解，裁罰須能夠真正遏制未來之違法行為，方具嚇阻性。裁罰須與違法行為整體相當，以符合比例。

就該案而言，綜合考量愛爾蘭 DPC 所認定之違反情事、加重事由以及裁罰對象之年營業額，裁罰決定草案所定之罰鍰金額範圍並未充分反映違法行為之嚴重性，且欠缺對 WhatsApp IE 之嚇阻性。

5. 重新評估罰鍰金額

EDPB 綜合前述分析，指示愛爾蘭 DPC 重新評估罰鍰金額，包括調整作為計算基礎之「年營業額」範圍及時點，計算罰鍰金額計算時，將年營業額及對各項規範之違反皆納入考量等。所科處之罰鍰金額應高於裁罰決定草案所定之罰鍰金額範圍，且應符合第 83 條第 1 項對有效性、合比例性與嚇阻性之要求。

二、簡析

「個人資料受保護之權利」乃「歐聯基本權利憲章」（Charter of Fundamental Rights of the European Union）第 8 條所肯認之一項獨立基本權。依該條規定，個人資料之處理，須為特定目的、基於當事人同意或其他法律依據，以公平方式為之；個資當事人享有存取及更正其個資之權利；且應以獨立機關監督遵循。因此，歐盟高度重視個人資料保護，並透過行政罰鍰之規範，促進個資保護法律之落實。

個資指令時代，歐盟就個人資料保護法規遵循事宜，並無統一之行政罰鍰標準，而是要求各會員國訂定裁罰規定，確保個資保護法規之落實¹⁶。GDPR 生效後，第 83 條成為具有直接適用效力之裁罰規定，各會員國主管機關均須遵守。

自 GDPR 前言第 148 點及歐盟法院相關見解¹⁷可知，行政罰鍰之目的係透過懲罰違法行為，強化對控管者、受託運用者等對個資保護規範之落實。或許是為落實此一立法目的，歐盟 EDPB 於其罰鍰計算

¹⁶ Directive 95/46/EC, Article 24.

¹⁷ C-300/21 - Österreichische Post (Préjudice moral lié au traitement de données personnelles), Opinion Of Advocate General (6 October 2022), <https://curia.europa.eu/juris/document/document.jsf?text=&docid=266842&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3719836>.

指引及有拘束力之決定中，皆強調罰鍰金額對違法行為人之有效性與阻嚇性，對行為人之規模（年營業額）之考量貫穿罰鍰計算之完整過程。

第二節 新加坡

一、規範重點

新加坡 PDPA 第 48J 規定科處行政罰鍰之條件、罰鍰金額上限及確定罰鍰金額之考量事由等。該條規定係 2020 年 PDPA 修正時所新增，並在 2022 年 10 月再次修正。現行第 48J 條的規範內容概述如下。

（一）法規內容要點

1. 主管機關科處裁罰之權力

PDPA 第 9C 章規定新加坡個人資料保護委員會（PDPC）之執法權，包括調查違法行為（第 48H 條）、糾正違法行為（第 48I 條）、科處行政罰鍰（financial penalty）（第 48J 條）、接受行為人之承諾（第 48L 條）等。

依據第 48J 條第 1 項，PDPC 如認定組織或人員¹⁸故意或過失違反 PDPA 之該條所列規範，得以書面針對該組織或人員科處罰鍰。

(1) 依第 48J 條第 1 項第 a 款，若組織違反下列個資保護規範，則可裁處罰鍰：

¹⁸ 新加坡 PDPA 並未明確區分「組織」與「人員」之差異，但「人員」多見於謝絕聯絡規範。依 PDPC 關於謝絕聯絡規範之指引，「人員」包括「個人、公司、協會或其他團體，無論是否具備法人資格」，此一概念與 PDPA 第 2 條第 1 項對「組織」之定義基本相同。See, Advisory Guidelines on the Do Not Call Provisions (1 February 2021), para 1.7, <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-on-the-DNC-Provisions-1-Feb-2021.pdf>.

- (a) 第 3 章之規範，包括遵守 PDPA，指派負責 PDPA 法遵事宜之專責人員，擬定並公開揭露 PDPA 遵循政策等義務；
- (b) 第 4 章之規範，包括個資蒐集、利用與揭露之法律依據、目的限制等；
- (c) 第 5 章之規範，包括個資當事人對資料之近用權與更正權等；
- (d) 第 6 章之規範，包括個資安全維護、儲存期間、境外傳輸等；
- (e) 第 6A 章之規範，包括個資侵害事故之通知與通報；或
- (f) 第 6B 章之規範，包括資料可攜相關權利（本章尚未生效）。

(2) 依第 48J 條第 1 項第 b 款，若人員違反謝絕聯絡(Do Not Call, DNC)之相關規範，亦可裁處罰鍰：

- (a) 第 i 目：第 9 章關於「謝絕聯絡登記簿(Do Not Call Register)」之規範，或
- (b) 第 2 目：第 48B 條第 1 項禁止使用流水號方式(dictionary attack)或電話號碼蒐集軟體(address-harvesting software)之規範。

第 48J 條第 2 項係刑事責任優先原則之體現，若 PDPA 已就某一違法行為規定刑事責任，則該違法行為應接受刑事處罰，PDPC 不得將其作為行政違法行為科處罰鍰。

2. 行政罰鍰之金額標準

PDPA 並未就行政罰鍰訂定下限，而是依違法行為之內容及行為人之性質，訂定不同之罰鍰金額上限：

(1) 依第 48 條第 3 項，針對第 48J 條第 1 項第 a 款所列違法行為（違反個資保護規範），其罰鍰金額上限如下：

(a) 若實施違法行為之組織的新加坡境內年營業額超過 1000 萬新加坡幣，且違法行為發生於《2020 年個人資料保護（修正）法》第 24 條生效後，則以該組織新加坡境內年營業額的 10% 為上限。

(b) 其他情形下，以 100 萬新加坡幣為上限。

(2) 依第 48 條第 4 項，針對第 48J 條第 1 項第 b 款第 i 目所列違法行為（違反謝絕聯絡登記簿相關義務），其罰鍰金額上限如下：

(a) 若個人實施違法行為，則以 20 萬新加坡幣為上限；

(b) 其他情形下，以 100 萬新加坡幣為上限。

(3) 依第 48 條第 4A 項，針對第 48J 條第 1 項第 b 款第 ii 目所列違法行為（違反流水號方式或電話號碼蒐集軟體使用禁止），其罰鍰金額上限如下：

(a) 若個人實施違法行為，則以 20 萬新加坡幣為上限；

(b) 若實施違法行為之人員（person）的新加坡境內年營業額（turnover）超過 2000 萬新加坡幣，且違法行為發生於《2020 年個人資料保護（修正）法》第 24 條生效後，則以該人員新加坡境內年營業額的 5% 為上限；

(c) 其他情形下，以 100 萬新加坡幣為上限。

(4) 依第 48J 條第 5 項，依同條第 3 項及第 4 項科處罰鍰時，如所違反之具體規範不同，得分別適用不同裁罰上限。

(5) 依第 48J 條第 5A 項，計算罰鍰金額法定上限之「新加坡境內年營業額」，以作出裁罰決定時，該組織或人員最近一次經查核之會計帳簿計算。

3. 個案裁罰金額之確定

第 48J 條第 6 項規定，PDPC 於確定個案中罰鍰金額時，須衡酌考量下列各項事由：

- (1) 違法行為之性質、重大性 (gravity) 與持續期間 (第 a 款)；
- (2) 違法行為所涉之個資類型與性質 (第 b 款)；
- (3) 該組織或人員是否因違法行為獲得經濟利益或避免經濟損失 (第 c 款)；
- (4) 該組織或人員是否採取措施減輕違法行為之影響，以及該行為之及時性與有效性 (第 d 款)；
- (5) 該組織或人員是否採行適足措施遵循 PDPA (第 e 款)；
- (6) 該組織或人員此前是否曾有違反 PDPA 之情事 (第 f 款)；
- (7) 該組織或人員是否遵循 PDPC 依第 48I 條或第 48L 條第 4 項所為之指示，補救或減輕違法行為之影響 (第 g 款)；
- (8) 考量落實遵循及嚇阻違法之需求，擬科處之行政罰鍰是否有效且合乎比例 (第 h 款)；
- (9) 行政罰鍰對該組織或人員之影響，包括其能否繼續正常從事活動 (第 i 款)；

(10) 其他相關因素（第 j 款）。

4. 科處罰鍰之程序

新加坡 PDPA 第 48K 條規定 PDPC 行使裁罰權應遵循之程序，具體包括：

- (1) 將擬作成之裁罰決定通知行為人，包括決定之內容及其理由。
- (2) 就擬作成之裁罰決定，給予行為人陳述意見之機會，並在通知中載明陳述意見之期間。陳述意見之期間不得少於 14 日，且得依行為人申請予以延長。
- (3) 作出最終裁罰決定前，須考量行為人之陳述意見。
- (4) 最終裁罰決定，須書面通知行為人，以及申訴人（如有）。
- (5) 最終裁罰決定須載明罰鍰繳納期，且不得少於 28 日。行為人得申請延長繳納期，或申請分期繳納。

（二）法規立法理由

新加坡 2012 年制定 PDPA，於該法第 29 條第 2 項第 d 款規定，PDPC 有權對違反該法第 3 章至第 6 章（主要內容與現行法相同）之行為，科處 100 萬新加坡幣以下之行政罰鍰。2020 年 11 月，新加坡國會通過 PDPA 修正案，大幅修正 PDPC 裁罰權之相關規範。

1. 修正草案之提出

該次修正案正式通過前，新加坡資通訊部（Ministry of Communications and Information, MCI）於 2020 年 5 月公布修正草案，

並舉辦公眾諮詢。修正草案第 17 條提出，從下列面向修正 PDPA 第 29 條關於行政罰鍰之規範¹⁹：

- (1) 對於違法行為之範圍，除原本已有規範的第 3 章至第 6 章外，亦納入第 9 章與第 9A 章（流水號方式或電話號碼蒐集軟體之使用禁止）。
- (2) 對於罰鍰之上限，導入浮動式裁罰上限，若違法行為人之年營業額超過 1000 萬新加坡幣，以其年營業額之 10% 為罰鍰金額上限；其他情形下，仍以 100 萬新加坡幣為上限。

針對罰鍰上限之修正，MCI 於其公眾諮詢說明文件中指出，此等修正目的在於強化罰鍰之嚇阻作用，並使 PDPC 能夠更靈活地依據違法行為之情節與嚴重性確定罰鍰金額。此外，調高後的罰鍰上限更貼合歐盟、澳洲等其他國家或地區之個資保護裁罰水準，就新加坡國內法制而言，較高之罰鍰上限也與競爭法等法規相一致²⁰。

2. 依公眾諮詢意見調整修正草案

2020 年 10 月，MCI 與 PDPC 對公眾諮詢意見作出回應。MCI 指出，針對罰鍰上限之修正，約三分之一的回應意見認為，在經濟因疫

¹⁹ MCI of Singapore, Public Consultation on the Draft Personal Data Protection (Amendment) Bill, Personal Data Protection (Amendment) Bill 2020, Section 17, <https://www.mci.gov.sg/public-consultations/public-consultation-items/public-consultation-on-the-draft-personal-data-protection-amendment-bill>.

²⁰ MCI of Singapore, Public Consultation on the Draft Personal Data Protection (Amendment) Bill, Public Consultation Document, para. 59, <https://www.mci.gov.sg/public-consultations/public-consultation-items/public-consultation-on-the-draft-personal-data-protection-amendment-bill>.

情而面臨下行壓力的情形下，提升罰鍰上限恐不適當。部分回應意見認為，修正後罰鍰上限之生效，應設適當準備期間（sunrise period）。此外，亦有回應意見認為，修正後罰鍰上限所稱之「年營業額」，應係「新加坡境內的年營業額」。

對於前述公眾諮詢意見，MCI 表示，將考量整體經濟環境，進一步酌調行政罰鍰法制。PDPC 表示，罰鍰金額上限提高後，其仍將繼續以審慎態度，綜合考量個案違法行為嚴重性、所造成影響、行為人責任程度、嚇阻違法之需要、罰鍰合比例性及其他各項因素，確定適當之罰鍰金額。

MCI 與 PDPC 並說明，為提升監理措施之明確性與可預見性，其將在 PDPA 中，調整罰鍰金額之加重或減輕事由提供例示。此外，為確保罰鍰上限符合比例，MCI 與 PDPC 將針對違反個資保護規範與違反謝絕聯絡規範分別設定不同上限，並將「年營業額」明確為「新加坡境內的年營業額」²¹。

3. 修正案之正式通過

2020 年 11 月 2 日，新加坡國會正式通過 PDPA 修正案，即《2020 年個人資料保護（修正）法》（以下稱 2020 年修正案）。該法第 23 條與第 24 條對 PDPC 科處罰鍰之權力進行二階段修正。

(1) 2020 年修正案第 23 條

²¹ MCI of Singapore, Closing Note to the Public Consultation on draft Personal Data Protection (Amendment) Bill including related amendments to the Spam Control Act (05 Oct 2020), [https://www.mci.gov.sg/public-consultations/public-consultation-items/closing-note-to-pc-on-draft-pdp-\(amendment\)-bill-including-related-amendments-to-spam-control-act](https://www.mci.gov.sg/public-consultations/public-consultation-items/closing-note-to-pc-on-draft-pdp-(amendment)-bill-including-related-amendments-to-spam-control-act).

2020 年修正案第 23 條刪除 PDPA 第 29 條關於 PDPC 科處糾正措施（包括行政罰鍰）之規定，並新增 PDPA 第 48J 條，作為 PDPC 科處罰鍰權力之專門規範。第 23 條之修正，自 2021 年 2 月 1 日起生效²²。

與原本第 29 條相比，該條對 PDPC 罰鍰權之修正如下：

- (a) 新增第 48J 條第 1 項，將第 6A 章、第 6B 章、第 9 章，以及第 9A 章的第 48B 條第 1 項納入違法行為之範圍。
- (b) 新增第 48J 條第 3 項，明定違反個資保護規範（原本第 3 章至第 6 章，以及新增之第 6A 章與 6B 章）之罰鍰上限，仍為 100 萬新加坡幣，與原本第 29 條第 2 項第 d 款相同。
- (c) 新增第 48J 條第 4 項，規定違反謝絕聯絡規範（第 9 章及第 48B 條第 1 項）之罰鍰上限，其中個人行為人之罰鍰上限為 20 萬新加坡幣，其他情形之上限為 100 萬新加坡幣。
- (d) 新增第 48J 條第 5 項，明定依同條第 3 項及第 4 項科處罰鍰時，如所違反之具體規範不同，得分別適用不同裁罰上限。
- (e) 新增第 48J 條第 6 項，明定確定個案罰鍰金額時應衡酌考量之各項事由。

由上可知，經 2020 年修正案第 23 條修正後，PDPA 雖針對違反個資保護規範與違反謝絕聯絡規範分別設定不同上限，並增列調整罰鍰金額之衡酌事由，但未導入浮動上限制度。

²² MCI of Singapore, Personal Data Protection (Amendment) Act 2020 (Commencement) Notification 2021 (27 January 2021), <https://sso.agc.gov.sg//SL/S60-2021?DocDate=20210129>.

(2) 2020 年修正案第 24 條

2020 年修正案第 24 條對 PDPA 新增之第 48J 條作出進一步修正，正式導入浮動上限制度。第 24 條之修正，自 2022 年 10 月 1 日起生效²³。

(a) 修正第 48J 條第 3 項，針對違反個資保護規範之行為，若行為人的新加坡境內年營業額超過 1000 萬新加坡幣，則以其年營業額之 10% 為罰鍰上限。

(b) 修正第 48J 條第 4 項、新增第 48J 條第 4A 項，針對違反 PDPA 第 48B 條第 1 項流水號方式或電話號碼蒐集軟體使用禁止之行為，若行為人的新加坡境內年營業額超過 2000 萬新加坡幣，則以其年營業額之 5% 為罰鍰上限。

(c) 新增第 48J 條第 5A 項，明定「新加坡境內年營業額」之計算依據。

(三) 實務運作標準

針對 PDPA 之執法事宜，PDPC 依 PDPA 第 65 條授權，針對執法事項訂定《個人資料保護（執法）細則》（Personal Data Protection (Enforcement) Regulations 2021），規定 PDPC 得公布科處罰鍰之決定²⁴。PDPC 並依 PDPA 第 49 條授權，訂定《執行資料保護規範之諮詢指引》（以下稱執法諮詢指引），說明其行使行政執法權時，對 PDPA 相關條款之解釋。此外，PDPA 並訂定《積極執法指引》，說明其執

²³ MCI of Singapore, Personal Data Protection (Amendment) Act 2020 (Commencement) Notification 2022 (27 September 2022), <https://sso.agc.gov.sg//SL/S767-2022>.

²⁴ Personal Data Protection (Enforcement) Regulations 2021, Section 18.

法策略，2022 年 10 月 1 日浮動上限制度生效時，PDPC 再次修正後兩部指引，說明其將如何適用最新修正的第 48J 條科處罰鍰。

1. 裁罰金額之計算步驟

PDPC 以積極執法指引說明，其在科處罰鍰時，將首先評估違法行為之性質，評估僅命令採取糾正措施，是否足以有效補救違法狀態。行政罰鍰之目的在於確保遵循及嚇阻違法。若依違法行為之嚴重程度，PDPC 認為有必要時，將考慮科處罰鍰。

PDPC 以下列方式確定個案罰鍰金額：

(1) 依據損害 (harm) 與有責性 (culpability) 原則，基於第 48J 條所列事由，評估個案之違法行為：

(a) 損害相關事由包括受影響之個資當事人數目、受影響之個資類別、違法行為之持續期間等。PDPC 將據此確定違法行為所涉損害之程度。

(b) 有責性相關事由涉及行為人之違法行為。PDPC 將考慮違法行為之性質，以及該行為人對 PDPA 之整體遵循狀況。

(2) 評估其他加重或減輕事由，酌調行政罰鍰金額，相關事由包括但不限於：

(a) 該組織或人員是否採取措施減輕違法行為之影響，以及該行為之及時性與有效性；

(b) 該組織或人員此前是否曾有違反 PDPA 等法規之情事；

- (c) 是否主動承認違法，包括是否透過「快速決定程序」
(Expedited Decision Procedure, EDP)²⁵表示願負責任；
- (d) 是否配合 PDPC 調查；
- (e) 該組織或人員是否為初犯。

(3) 考量行政罰鍰對該組織或人員可能造成之影響，以及罰鍰對於落實遵循與嚇阻違法之合比例性與有效性，酌調罰鍰金額。

2. 個案裁罰金額之衡酌方式

PDPC 於執法諮詢指引中，彙整過往裁罰案例，對第 48J 條第 6 項所列各項事由提供例示說明。

(1) 違法行為之性質、重大性與持續期間

- (a) 未經授權之揭露行為僅涉及 1 名無權接收者，且僅持續 10 分鐘，屬於減輕事由²⁶。
- (b) 組織知悉其託運單追蹤頁面可用於未經授權存取個資，但在知悉後 2 年多內，皆未採取糾正措施，以致最終發生資料外洩，屬於加重事由²⁷。

²⁵ 「快速決定程序」係 PDPC 行政調查程序之一類。此類程序中，被調查之行為人透過主動承認違法並承擔責任，使行政調查得以於較短時間內結束。See, PDPC, Guide on Active Enforcement (1 October 2022), 23-25.

²⁶ Institute of Singapore Chartered Accountants [2018] SGPDPC 28, Decision, para 22.

²⁷ Ninja Logistics Pte Ltd [2019] SGPDPC 39, Decision, para 18.

(c) 組織遭外流之密碼已長達 10 年未作變更，且組織未能及時偵測到入侵行為，以致利用該密碼未經授權存取個資已長達 2 年，屬於加重事由²⁸。

(2) 違法行為所涉之個資類型與性質

(a) 敏感個資（特別是醫療紀錄與保險金額）遭到外洩，屬於加重事由²⁹。

(b) 外洩事件涉及眾多個資當事人，且資料敏感度較高，屬於加重事由³⁰。

(c) 組織因系統編程錯誤，導致 426 名當事人的登入帳號、Email 地址、收件地址和手機號碼遭外洩。PDPC 考量所涉個資之數量與類別，認為屬減輕事由³¹。

(3) 該組織或人員是否因違法行為獲得經濟利益或避免經濟損失

(a) 組織出售個資並獲取利潤，屬於加重事由³²。

(4) 該組織或人員是否採取措施減輕違法行為之影響，以及該行為之及時性與有效性

²⁸ SPH Magazines Pte Ltd [2020] SGPDPC 3, Decision, para 13.

²⁹ Aviva Ltd [2018] SGPDPC 4, Decision, para 30.

³⁰ Singapore Health Services Pte. Ltd. and Integrated Health Information Systems Pte. Ltd. [2019] SGPDPC 3, Decision, para 139.

³¹ Option Gift Pte Ltd [2019] SGPDPC 10, Decision, para 9.

³² Sharon Assya Qadriyah Tang [2018] SGPDPC 1, Decision, para 32; Amicus Solutions Pte. Ltd. and Ivan Chua Lye Kiat [2019] SGPDPC 33, Decision, paras 52 & 53.

(a) 組織於知悉外洩事故後，及時採取措施有效修補導致外洩之系統漏洞，屬於減輕事由³³。

(b) 組織於知悉外洩事故後 11 小時內，採取臨時措施減輕事故影響，屬於減輕事由³⁴。

(5) 該組織或人員是否採行適足措施遵循 PDPA

(a) 組織已訂定並公布個資保護政策，且每年皆由內部法遵團隊（在外部顧問之協助下）執行內部稽核，評估系統權限風險、資料完整性風險和生產環境配置風險，屬於減輕事由³⁵。

(b) 組織為防範網路安全風險，定期執行滲透測試、弱點測試及程式碼審查，屬於減輕事由³⁶。

(6) 該組織或人員此前是否曾有違反 PDPA 之情事

(a) 組織已是一年內再次違反 PDPA，且違法行為之事實模式相同，屬於加重事由³⁷。

(b) 組織此前已發生類似違法行為，屬於加重事由³⁸。

³³ Zero1 Pte. Ltd. and XDEL Singapore Pte. Ltd. [2019] SGPDPC 37, Decision, para 26.

³⁴ Singapore Telecommunications Limited [2019] SGPDPC 49, Decision, para 14.

³⁵ Propnex Realty Pte Ltd [2017] SGPDPC 1, Decision, para 32.

³⁶ ComGateway (S) Pte. Ltd. [2017] SGPDPC 19, Decision, para 37.

³⁷ Aviva Ltd and Toh-Shi Printing Singapore Pte Ltd [2016] SGPDPC 15, Decision, para 38.

³⁸ Aviva Ltd [2018] SGPDPC 4, Decision, para 30.

(7) 該組織或人員是否遵循 PDPC 依第 48I 條或第 48L 條第 4 項所為之指示，補救或減輕違法行為之影響

(a) 目前尚無案件出現此一事由，但 PDPC 認為，若組織未能遵守 PDPC 對該違法行為已命令之糾正措施，得作為加重事由。

(8) 考量落實遵循及嚇阻違法之需求，擬科處之行政罰鍰是否有效且合乎比例

(a) Singapore Health Services Pte. Ltd. 和 Integrated Health Information Systems Pte. Ltd. 個資外洩事件中，PDPC 考量該案係當時新加坡最嚴重之外洩事件，且該兩家公司之防範與因應措施顯有不足，對兩家公司合計裁罰 100 萬新加坡幣，係依當時法律所能裁罰之最高金額³⁹。

(b) 組織未經當事人同意出售其個資，並藉此營利，係 PDPA 所欲防制之行為，屬加重事由。且 PDPC 於確定罰鍰金額時，得考量組織因此所獲收益之金額⁴⁰。

(9) 行政罰鍰對該組織或人員之影響，包括其能否繼續正常從事活動

³⁹ Singapore Health Services Pte. Ltd. and Integrated Health Information Systems Pte. Ltd. [2019] SGPDPC 3, Decision, para 138.

⁴⁰ Amicus Solutions Pte. Ltd. and Ivan Chua Lye Kiat [2019] SGPDPC 33, Decision, paras 54 & 55.

(a) 組織因遭受詐欺，財務狀況嚴重不良，且唯一股東年事已高，但仍計劃大幅縮減業務規模後繼續經營，屬於減輕事由⁴¹。

(b) 組織為家庭型商號且營收較低，無力負擔罰鍰，屬於減輕事由⁴²。

(10) 其他相關因素

(a) 組織的業務涉及大量個資，且個資之洩漏可能給當事人造成嚴重損害或痛苦，屬於加重事由⁴³。

(b) 組織雖辯稱其行為係為響應政府推動中小企業（SME）數位化之目標，然 PDPC 認為，此並不構成減輕事由。蓋中小企業須自數位化進程開始時，即採行良好之資料管理和個資保護措施，且中小企業無須負擔過高成本，即可採行該等措施⁴⁴。

(c) 組織在外洩所涉之資料庫遭刪除後，仍透過分析 Email 往來紀錄，盡力確定受影響之使用者 Email 數量，屬於減輕事由⁴⁵。

⁴¹ O2 Advertising Pte. Ltd. [2019] SGPDP 32, Decision, paras 12 & 13.

⁴² Advance Home Tutors [2019] SGPDP 35, Decision, paras 27 & 30.

⁴³ Aviva Ltd [2018] SGPDP 4, Decision, para 30.

⁴⁴ DS Human Resource Pte. Ltd. [2019] SGPDP 16, Decision, para 14.

⁴⁵ Creative Technology Ltd [2020] SGPDP 1, Decision, para 13.

（四）案例

2018 年 7 月，新加坡發生當時史上最嚴重之個資外洩事件，約 150 萬名病患之個人資料及 16 萬名病患的醫療紀錄遭外洩。該外洩起因於公共醫療機構 Singapore Health Services Pte. Ltd.（以下稱 SingHealth）的電子病歷系統遭駭客攻擊，而遭攻擊的系統係由醫療資訊系統供應機構 Integrated Health Information Systems Pte. Ltd.（以下稱 IHiS）負責管理。2019 年，新加坡 PDPC 針對該個資外洩事件，對 SingHealth 和 IHiS 兩家公司合計裁罰 100 萬新加坡幣，此係依當時法律所能裁罰之最高金額。該裁罰決定雖作出於 2020 年修正案通過之前，然因新加坡 PDPC 執法舉措之一貫性，其於該案中對罰鍰金額之衡酌，仍具參考性。

1. 事實背景

SingHealth 和 IHiS 都是新加坡衛生部（Ministry of Health）為提供公共醫療服務而投資設立之公司。SingHealth 負責營運公共醫療機構，而其資訊系統則依新加坡衛生部要求，由 IHiS 集中管理與維護。2018 年 7 月 20 日，新加坡資通訊部與衛生部聯合公開該外洩事件，並成立調查委員會。PDPC 亦於接獲民眾申訴後，對 SingHealth 和 IHiS 的個資法違法情事啟動調查。

PDPC 啟動調查後，SingHealth 和 IHiS 皆同意配合，以加速調查程序。兩家公司並主動承認其違反情事，接受 PDPC 之認定結論。

經調查，該事件歷程如下：

- (1)駭客自 2017 年 8 月起即已啟動攻擊，首先透過釣魚 Email 等方式，入侵員工之工作電腦，並藉此取得管理員帳號等，進而透過所掌握之帳號，存取 SingHealth 所屬醫院之舊伺服器。

遭入侵的舊伺服器已規劃停用，當時正處於新舊交接之過渡期。

(2)駭客自 2018 年 5 月底起，多次嘗試透過舊伺服器存取新伺服器，但皆未成功。

(3)2018 年 6 月，IHiS 獲知異常存取嘗試，並與 SingHealth 成立因應小組，但未採取積極作為。

(4)2018 年 6 月 26 日，駭客透過舊伺服器，獲知新伺服器之登入帳密，並成功登入。

(5)2018 年 6 月 27 日至 7 月 4 日間，駭客取走大量資料，包括姓名、身分證號碼、地址、性別、生日、處方紀錄等。

(6)2018 年 7 月 4 日，IHiS 員工獲知異常存取示警，並通知公司啟動因應程序，移除從舊伺服器存取新伺服器之權限。

(7)IHiS 於 2018 年 7 月 10 通報新加坡網路安全局(Cyber Security Agency, CSA)，並配合 CSA 採取因應措施。

2. 罰鍰金額之衡酌

2019 年 1 月，新加坡 PDPC 對該案作出裁罰決定，認為 SingHealth 和 IHiS 違反當時新加坡 PDPA 第 24 條關於個資安全保護之規範。依當時同法第 29 條，PDPC 有權科處糾正措施，包括最高 100 萬新加坡幣之行政罰鍰。

PDPC 在計算行政罰鍰時，認為存在下列加重事由：

(1)本案是新加坡歷史上規模最大的個資外洩事故，受影響的個資當事人總數高達近 150 萬人。

- (2)雖然實際外洩人數近 150 萬人，但從駭客攻擊之資料庫規模觀察，超過 501 萬人的個資安全遭受威脅，且涉及高度機密性的醫療資料。SingHealth 和 IHiS 對個資安全保護不足情節更為嚴重。
- (3)駭客取得 15.9 萬人的處方資料，且從該等資料可推知所患疾病，這可能是相當嚴重或私密的疾病。

針對 SingHealth 之罰鍰，SingHealth 在其陳述意見中提出，其已採取諸多安全措施，足以對其委外廠商 IHiS 施以適當監督，因此請求 PDPC 考量比例原則，降低罰鍰金額。PDPC 對此認為，依法律要求之標準採取適當安全措施並不足以構成減輕或免除行政責任之事由。但就本案而言，SingHealth 和 IHiS 存在下列減輕事由：

- (1)SingHealth 和 IHiS 皆主動明確承認其違法行為，接受 PDPC 之認定，並同意與 PDPC 配合，加速調查和責任認定。
- (2)SingHealth 和 IHiS 已配合調查。
- (3)SingHealth 和 IHiS 在個資事故發生後，立即採取有效因應措施。
- (4)SingHealth 自身也是專業駭客入侵行為之受害者。
- (5)SingHealth 因國家公共醫療政策要求，必須將其 IT 基礎設施委由 IHiS 集中營運。

PDPC 綜合考量上述事由，對 SingHealth 科處 75 萬新加坡幣罰鍰，對 IHiS 科處 25 萬新加坡幣罰鍰。

二、簡析

新加坡 PDPA 自訂定之時，即已規定行政罰鍰之固定上限。其修正 PDPA、導入雙軌制罰鍰規範之目的，在於強化罰鍰之嚇阻作用，為 PDPC 採行執法措施提供更多裁量空間，並使新加坡個資法之罰鍰水準與歐盟、澳洲等其他國家或地區相一致。

為減緩修法條文對社會及產業之衝擊，新加坡之修法歷程採分階段進行模式，以第一階段較具過渡期性質，細化行政罰鍰之科處程序及審酌事由規定，但未實質提高罰鍰金額上限；第二階段則完整落實修法目的，導入雙軌制罰鍰規範，對大型組織實體提高罰鍰金額上限。立法機關一次性通過各階段之修正條文後，將施行日期交由行政主管機關訂定。實務執行中，從修正條文經國會通過，到雙軌制罰鍰正式施行，歷時將近兩年。且個資保護主管機關 PDPC 於各階段修正條文施行之當日，即一併發布修正（更新）後之配套子法規及執法措施相關指引，使業者可迅速獲得主管機關執法策略之實務資訊，強化執法措施之可預見性。新加坡之前述措施，可作為修法進程之參考。

第三節 南韓

一、規範重點

現行南韓個資法就違法行為以刑罰為主，罰鍰（課徵金）及行政罰款（過怠料）⁴⁶等行政罰為輔，主要罰則明定於第 70 條以下，裁罰內容分有自由刑、財產刑（罰金）及行政罰款，至於罰鍰之規定則散落於第 28 條之 6、第 34 條之 2、第 39 條之 15 等條文。

2020 年南韓個資法引進假名情報、將舊「情報通信網利用促進暨情報保護等相關法律」（以下稱「情報通信網法」）裁罰「情報通信服務提供者」⁴⁷侵害個資之違法行為相關條文併入現行個資法，以及賦予主管機關即「個人情報保護委員會」（以下稱委員會）得依法逕向違反義務人科處罰鍰，透過修法增加行政罰（包含罰鍰及行政罰款）於個資法中的比重，本研究將以個資法中之罰鍰為主軸，其相關法規內容、立法理由、實務運作、案例等探討現行南韓個資法就罰鍰之運作，並介紹未來南韓個資法裁罰基準的修法方向。

（一）法規內容要點

依現行南韓個資法第 7 條之 9 第 1 項第 8 款規定，保護委員會得以會議議決罰鍰（課徵金）的相關裁處，並於同法第 28 條之 6、第 34

⁴⁶ 課徵金（과징금）與過怠料（과태료）均屬於行政處分，前者係指違反行政法上的特定義務，行政機關對違反義務者為金錢上的制裁，並具有追繳不法利得性質，至於過怠料與刑罰上的微罪罰金相似，通常用於未履行輕微的行政義務，該未履行義務無法以刑法制裁，受裁罰人未繳納過怠金時，行政機關得以強制徵收程序為執行。

⁴⁷ 「情報通信服務提供者」（정보통신서비스 제공자）依「情報通信網利用促進暨情報保護等相關法律」（簡稱為情報通信網法）第 2 條第 3 款規定，係指「電子通信產業法」第 2 條第 8 款規定之電信業者，及以營利為目的利用電信業者之電信業務以提供個資或居間提供個資者，亦即除提供網際網路服務之電信業者外，有以營利為目的而利用網路提供個資或為居間行為者均屬之。

條之 2、第 39 條之 15 分別規定各違法行為應裁處之罰鍰標準，茲將各該條文羅列於下：

1. 第 28 條之 6（對處理假名情報課賦課徵金）

- (1) 個人情報管理者違反第 28 條之 5 第 1 項規定，以識別特定個人為目的而處理情報時，保護委員會得對其課賦整體銷售總額百分之三以下之課徵金。但無整體銷售總額或計算顯有困難時，得依大統領令規定，以 4 億韓圓或資本額百分之三，課賦兩者之最高金額以下之課徵金。
- (2) 有關課徵金之課賦、徵收等必要事項，準用第 34 條之 2 第 3 項至第 5 項的規定。

2. 第 34 條之 2（課徵金等）

- (1) 個人情報處理者於處理住民登錄號碼有遺失、竊取、洩漏、變造及毀損之情事時，保護委員會得課賦、徵收 5 億元以下之課徵金。但個人情報處理者為避免住民登錄號碼被遺失、竊取、洩漏、變造及毀損，已依第 22 條第 3 項設置安全維護必要措施時，不在此限。
- (2) 保護委員會於第 1 項課賦課徵金時，應評估下列各款事項
 - (a) 履行第 24 條第 3 項安全維護必要措施之努力程度；
 - (b) 住民登錄號碼被遺失、竊取、洩漏、變造及毀損之程度；
 - (c) 是否履行後續措施以防止侵害擴散
- (3) 如未依第 1 項於繳納期間內繳納課徵金者，自繳納截止日次日始至繳納日前一日止，保護委員會於課徵金之年利率百分

之六範圍內依大統領令徵收滯納金。此時，滯納金之徵收期限不得超過 60 個月。

- (4) 如未依第 1 項於繳納期間內繳納課徵金者，保護委員會應限期催繳，若仍未於該期間內繳納課徵金及第 2 項所定之滯納金，依國稅滯納處分之案例徵收。
- (5) 關於課徵金之課賦、徵收等其他必要事項以大統領令定之。

3. 第 39 條之 15（課徵金之課徵等相關特例）

- (1) 情報通信服務提供者有符合下列各款之一之行為時，保護委員會得依違法行為對情報通信服務提供者等課賦該相關銷售額百分之三以下之課徵金。
 - (a) 違反第 17 條第 1 項、第 2 項、第 18 條第 1 項、第 2 項及第 19 條（包含依第 39 條之 14 規定準用時），有個人情報之利用、提供時；
 - (b) 違反第 22 條第 6 項（包含依第 39 條之 14 規定準用時）未取得法定代理人同意即蒐集 14 歲以下兒童之個人情報；
 - (c) 違反第 23 條第 1 項第 1 款（包含依第 39 條之 14 規定準用時）未取得當事人同意即蒐集敏感情報；
 - (d) 疏於進行第 26 條第 4 項（包含依第 39 條之 14 規定準用時）所定之管理、監督及教育致特別受託者有違反本法規定時；
 - (e) 未依第 29 條設置措施（樹立內部管理計畫除外）之規定（包含依第 39 條之 14 規定準用時）致使用者之個人情報有遺失、竊取、洩漏、偽造、變造及毀損之情形；

- (f) 違反第 39 條之 3 第 1 項（包含依第 39 條之 14 規定準用時）未取得當事人同意即蒐集個人情報時；
 - (g) 違反第 39 條之 12 第 2 項本文（包含依同條第 5 項準用時）未取得當事人同意即向國外提供當事人之個人情報
- (2) 根據第 1 項規定被課賦課徵金之情報通信服務提供者等，有拒絕提出核算銷售額資料或提出虛假資料時，以與該情報通信服務提供者等規模相似之情報通信服務提供者等之財務報表等會計資料及註冊者數暨使用費用等營業現況資料為證據，推定其銷售額。但無銷售額或覈算銷售額有困難時，得課賦依大統領令所定之 4 億韓圉以下之課徵金。
- (3) 保護委員會欲依第 1 項課賦課徵金時，應評估下列各款事項
- (a) 違法行為之內容暨程度；
 - (b) 違法行為之期間暨次數；
 - (c) 依違法行為而取得利益之規模
- (4) 第 1 項課徵金經第 3 項評估後核定，該具體之核定基準與核定程序應以大統領令定之。
- (5) 根據第 1 項應繳納課徵金而未於繳交期間內繳納者，保護委員會應加徵自繳納期間屆滿次日起算課徵金之百分之六年利率之滯納金。
- (6) 根據第 1 項應繳納課徵金者有未於繳交期間內繳納之情形，保護委員會應定期限催繳，如於該指定期限內仍未繳納課徵金及第 5 項之滯納金，則依國稅滯納處分案例徵收。

(7)有法院判決等事由而有返還第 1 項所課賦之課徵金時，自繳納課徵金之日起至返還當日止之期間內，應評估金融公司之存款利率等，依大統領令定之利率計算並返還滯納金。

(8)雖符合第 7 項之規定，惟根據法院判決取消該課賦課徵金處分，而判決理由中有課賦新的課徵金時，以當初已繳納之課徵金扣抵新的課徵金，並僅就剩餘額計算返還滯納金併予返還。

前揭各條文雖均規定於個資法中，惟其適用對象、違法行為及裁罰內容略微不同。以適用對象為例，第 28 條之 6 及第 34 條之 2 規定適用對象為「個人情報處理者」、第 39 條之 15 規定適用對象為「情報通信服務提供者」；在違法行為部分，第 28 條之 6 及第 34 條之 2 較為單純，前者係「個人情報處理者」以識別特定個人為目的而處理假名情報，後者專指「個人情報處理者」在處理住民登錄號碼（相當於身分證字號，如為外國人則為外國人登錄證號碼）有遺失、竊取、洩漏、變造及毀損之情事時，而第 36 條之 15 乃將修法前「情報通信網法」第 64 條之 3 規定併入南韓個資法，與前揭第 28 條之 6 及第 34 條之 2 兩條僅規範特定行為有異。

第 36 條之 15 所裁罰之行為係針對「情報通信服務提供者」於違反個資處理基本原則，例如未經同意蒐集及利用、提供予第 3 方為目的之外之利用、未經同意蒐集敏感個資、未設置安全措施致個資受侵害等，其等均屬修法前「情報通信網法」之裁罰規定，故第 36 條之 15 可視為個資法的特別規定，對「情報通信服務提供者」核定裁罰時應優先適用。

至於裁罰額，第 28 條之 6 處理假名情報係以「整體」銷售額⁴⁸百分之三以下為核算，第 34 條之 2 就處理住民登錄號碼部分，其罰鍰標準非以銷售額定之，係採 5 億韓幣以下之標準；而第 36 條之 15「情報通信服務提供者」違反個資處理基本原則部分，則核定罰鍰係以「與該違法行為相關」之銷售額百分之三為基準，因各裁罰基準不同，所遵循之實務操作標準亦均不同，將敘明於後。

（二）法規立法理由

第 28 條之 6 係 2020 年 2 月 4 日修正個資法（本研究撰擬時適用之現行法），引進假名情報制度所設，其立法理由為對違反之個人情報處理者課賦整體銷售額百分之三以下之罰鍰以避免任何人為識別特定個人而處理假名情報。

第 34 條之 2 係 2013 年 8 月 6 日修正個資法時新制定之規定，其立法理由為住民登錄號碼大量外流及惡意使用頻繁，現行法（2013 年 8 月 6 日修正前之個資法）難以對造成外流事件的大型企業追究民刑事責任，因此藉由原則禁止處理住民登錄號碼、住民登錄號碼有滅失、竊取、外流、變造、毀損等情事時，課賦韓幣 5 億元以下之罰鍰，以明確防止住民登錄號碼外流，強化企業對個人資料保護之職責。

第 39 條之 15 係源自舊「情報通信網法」第 64 條之 3，其立法理由為企業間為維持客戶而互相競爭，持有的客戶資料急劇增加致大量外流的事件頻傳，僅有行政罰款及刑罰等制裁手段已無法預防個資外流問題的發生，藉由課賦罰鍰的制裁方式可進一步對不法蒐集、利

⁴⁸ 銷售額係指於銷售商品及提供服務之收入總額中扣除折讓或退款後之淨額（參考憲法裁判所 2020 헌바 259 判決文第 7 頁）。

用及洩漏個人資料，或未設置保護措施等之違反義務人，追繳其違法行為之不法利得，預期得有效減少個人資料侵害及外流事件，增進個資當事人的權益。該條文最初課賦罰鍰基準為「與該違法行為相關」銷售額百分之一以下核定罰鍰，若未設置保護措施致個人資料洩漏時則課賦韓幣 1 億元以下之罰鍰⁴⁹。復銀行及信用卡公司持續發生逾 1 億筆個人資料外流事件，且個資透過網路大量外流，2 次侵害的可能性極高，認有必要強化處罰以因應，故 2014 年 5 月 28 日修正該裁罰條文，將「『與該違法行為相關』銷售額百分之一以下」修正為「『與該違法行為相關』銷售額百分之三以下」⁵⁰。而 2020 年為配合個資法修正，舊「情報通信網法」有關個人資料保護相關規定併入個資法，乃刪除舊「情報通信網法」第 64 條之 3，於個資法新制定第 39 條之 15。

（三）實務運作標準

1. 第 28 條之 6

第 28 條之 6 規定專指處理假名情報之違法行為，其裁罰基準依南韓個資法施行令第 29 條之 6 規定「①本法第 28 條之 6 第 1 項所定之銷售額，以該個人情報處理者之前 3 個事業年度之年均銷售額為之。但該事業年度之始日至今未滿 3 年，自該事業始日起至前事業年度末日止之年均銷售額換算之，若該事業年度為事業開始之情形，以該事業始日起至違法行為之日止之銷售額作為年銷售額換算之。②本法第 28 條之 6 第 1 項但書『以大統領令規定』指符合下列任一款之

⁴⁹ 參 2008 年 6 月 13 日法律第 9119 號第 64 條之 3 條文內容。

⁵⁰ 參 2014 年 5 月 28 日法律第 12681 號第 64 條之 3 條文內容。

情形 1. 尚未開始營業或因營業中斷等事由致無營業實績之情形 2. 因災害等致核算銷售額之資料減失或毀損等，難以客觀核算銷售額之情形。③保護委員會為計算第 1 款規定之銷售額，有需要財務報表等資料之情形，得要求個人情報處理者於 20 日以內提交相關資料。④本法第 28 條之 6 第 1 項規定之課徵金核算基準及核算程序同附表 1。」。

復參南韓個資法施行令附表 1 即「課徵金之核算基準及核算程序（第 29 條之 6 第 4 項相關）」（以下稱附表 1）所載，依個資法第 28 條之 6 第 1 項核定罰鍰時，應以施行令第 29 條之 6 第 1 項⁵¹規定之年均銷售額，依附表 1 第 2 點所載核算階段及核算方式進行，其順序為第一步驟：綜合評估違法行為致生之影響後核算金額、第二步驟：對該核算金額依情節認定有無加重、減輕之必要、第三步驟：對該核算金額依情節認定是否為加重、減輕之補充、第四步驟：決定應裁罰之罰鍰。

首先，第一步驟：綜合評估違法行為致生之影響後核算金額，係指根據違法行為之重大性區分裁罰額的核算比率，違法行為相當重大者，核算比率為 0.027、違法行為重大者，核算比率為 0.021、違法行為通常者，核算比率為 0.015，再以年均銷售額乘以各該核算比率產生核算金額；若符合施行令第 29 條之 6 第 2 項任一款情形者，依其違法行為之重大性核算：違法行為相當重大者，核算金額為 3 億 6 千

⁵¹ 施行令第 29 條之 6 第 1 項條文為「個人資料保護法第 28 條之 6 第 1 項規定之銷售額以該個人資料處理者前 3 個事業年度之年均銷售額為之。但該事業年度之始日至今未滿 3 年，自該事業始日起至前事業年度末日止之年均銷售額換算之，若該事業年度為事業開始之情形，以該事業始日起至違法行為之日止之銷售額作為年銷售額換算之。」。

萬韓幣、違法行為重大者，核算金額為 2 億 8 千萬韓幣、違法行為通常者，核算金額為 2 億韓幣；另依前揭標準產生初步核算金額前，仍應考量對違法行為重大性之故意、有無重大過失、有無營利目的、受害規模、個人資料有無對公眾外流，及因違法行為獲取之利益範圍等綜合評估以計算核算金額。

其次，第二步驟：對該核算金額依情節認定有無加重、減輕之必要，係指經第一步驟之核算金額，應依違法行為之存續期間及次數等情節判斷核算金額有無加重、減輕之必要，於必要時以百分之五十範圍內為加重或減輕。

第三步驟：對該核算金額依情節認定是否為加重、減輕之補充，係就經第二步驟為必要加重、減輕之核算金額，應視對個人資料保護努力程度、有無配合違法行為調查、有無主導違法行為等為整體考量，得於百分之五十範圍內為補充加重或減輕。

最後，第四步驟：決定應裁罰之罰鍰，係指對違法行為人為裁罰前得依相當情節再次確認得減輕或免除裁罰；就得減輕部分，乃委員會最終決定罰鍰前得考量違法行為人現實上負擔能力、違法行為發生後對個資當事人的侵害程度及賠償金額、違法行為人所屬產業或市場是否因經濟危機致顯著的變動或狀態持續惡化等，認經前三步驟核算金額過重時，得於該核算金額之百分之九十內為減輕，決定應裁罰之罰鍰。得免除裁罰部分，於符合違法行為人有給付不能、停止支付或資本虧損（Impairment of Capital）⁵²等事由認違法行為人客觀上無給付能力時、違法行為之內容及程度極其輕微、核算金額為小額、違法行為人有正當事由無法認知自己的行為違法時等任一情節時，委員會

⁵² 原文為「자본 잠식」，漢字為資本蠶食。

得免除裁罰。惟附表 1 僅係核算罰鍰的基本程序及方法，就違法行為重大性、加重及減輕之必要、加重及減輕之補充等判斷標準，附表 1 明文授權由保護委員會另行公告⁵³之。

2. 第 34 條之 2

第 34 條之 2 規定處理住民登錄號碼裁罰五億韓幣以下之罰鍰，此裁罰基準依個人資料保護法施行令第 40 條之 2 第 1 項適用同法附表 1 之 3，依附表 1 之 3 所載，決定裁罰原則係依個資法第 34 條之 2 第 2 項綜合評估所列各款事項所生之影響，核算程序為第一步驟：基本核算、第二步驟：第一次調整、第三步驟：第二次調整、第四步驟：決定應裁罰之罰鍰。

首先，第一步驟：基本核算，係指依違法行為之重大性區分，違法行為相當重大者，乃故意或重大過失導致 10 萬筆以上住民登錄號碼遺失、被竊、洩漏、變造或毀損等情形，核算金額為 3 億 5 千萬韓幣；違法行為重大者，乃故意或重大過失導致未滿 10 萬筆住民登錄號碼遺失、被竊、洩漏、變造或毀損等，抑或輕過失導致 10 萬筆以上住民登錄號碼遺失、被竊、洩漏、變造或毀損等情形，核算金額為 2 億 3 千萬韓幣；違法行為通常者，乃輕過失導致未滿 10 萬筆住民登錄號碼遺失、被竊、洩漏、變造或毀損等情形，核算金額為 1 億韓幣。

⁵³ 保護委員會於 2021 年 4 月 1 日發出「違反假名情報處理之過徵金基準制定案行政預告」公告：

<https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS061&mCode=C010010000&nttId=7242>（最後瀏覽日為 2023 年 4 月 19 日），向機關團體蒐集意見，目前尚未見該基準上線。

其次，第二步驟：第一次調整，係指得評估違法行為人依個資法第 24 條第 3 項規定履行安全維護必要措施之努力程度、有無規劃對策使侵害最小化等防止侵害擴散之後續措施等情節，判斷核算金額有無加重、減輕之必要，得於百分之五十範圍內為加重或減輕。

第三步驟：第二次調整，係於綜合考量違法行為之期間及次數、平時個人資料保護努力程度、有無配合違法行為調查、違法行為是否造成其他額外侵害等情節，得再於第二步驟經加重或減輕之核算金額之百分之五十範圍內為加重或減輕。

最後，第四步驟：決定應裁罰之罰鍰，係指於最終決定罰鍰前得依相當情節再次確認是否減輕或免除裁罰；就得減輕部分，乃委員會得考量違法行為人現實上負擔能力、違法行為發生後對個資當事人的侵害程度及賠償金額、違法行為人所屬產業或市場是否因經濟危機致顯著的變動或狀態持續惡化等，認經前三步驟核算金額過重時，得於該核算金額之百分之九十內為減輕，決定應裁罰之罰鍰。得免除裁罰部分，於符合違法行為人有給付不能、停止支付或資本虧損等事由認違法行為人客觀上無給付能力時、違法行為之內容及程度極其輕微、核算金額為小額、違法行為人有正當事由無法認知自己的行為違法時等任一情節時，委員會得免除裁罰。惟附表 1 之 3 僅係核算罰鍰的基本程序及方法，就違法行為重大性、加重及減輕等判斷標準，依個人情報保護委員會於 2022 年 10 月 20 日制定公布之「住民登錄號碼外流等相關課徵金課賦基準」⁵⁴，就故意及重大過失程度之判斷需通

⁵⁴ 「주민등록번호 유출 등에 대한 과징금 부과기준」，
<https://www.law.go.kr/LSW/admRulLsInfoP.do?admRulSeq=2100000215231>
(最後瀏覽日：2023 年 4 月 19 日)

盤考量違反目的、動機、因果關係等情事，以及第一次調整、第二次調整等加重及減輕之比重等，均有更細部之規定。

3. 第 39 條之 15

(1) 操作原則

第 39 條之 15 規定情報通信服務提供者有違法行為時，其裁罰基準依南韓個資法施行令第 48 條之 11 規定「①本法第 39 條之 15 第 1 項所定之銷售額，以與該情報通信服務提供者之違法行為相關的情報通信服務前 3 個事業年度之年均銷售額為之。但該事業年度之始日至今未滿 3 年，自該事業始日起至前事業年度末日止之年均銷售額換算之，若該事業年度為事業開始之情形，以該事業始日起至違法行為之日止之銷售額作為年銷售額換算之。②本法第 39 條之 15 第 2 項但書『以大統領令規定』指符合下列任一款之情形 1. 尚未開始營業或因營業中斷等事由致無營業實績之情形 2. 因災害等致核算銷售額之資料減失或毀損等，難以客觀核算銷售額之情形。③保護委員會為計算第 1 款規定之銷售額，有需要財務報表等資料之情形，得要求情報通信服務提供者於 20 日以內提交相關資料。④本法第 39 條之 15 第 4 項規定之課徵金核算基準及核算程序同附表 1 之 5。」。

復參南韓個資法施行令附表 1 之 5 即「課徵金之核算基準及核算程序（第 48 條之 11 第 4 項相關）」（以下稱附表 1 之 5）所載，依個資法第 28 條之 6 第 1 項核定罰鍰時，應綜合評估個資法第 39 條之 15 第 3 項各款即該違法行為所帶來的影響，並依附表 1 之 5 第 2 點所載核算階段及核算方式進行，其順序為第一步驟：綜合評估違法行為致生之影響後核算金額、第二步驟：對該核算金額依情節認定有無

加重、減輕之必要、第三步驟：對該核算金額依情節認定是否為加重、減輕之補充、第四步驟：決定應裁罰之罰鍰。惟經最終核算之裁罰額不得超過個資法第 39 條之 15 第 1 項及第 2 項規定之裁罰額。

首先，第一步驟：綜合評估違法行為致生之影響後核算金額，係指根據違法行為之重大性區分裁罰額的核算比率，違法行為相當重大者，核算比率為 0.027、違法行為重大者，核算比率為 0.021、違法行為通常者，核算比率為 0.015，再以年均銷售額乘以各該核算比率產生核算金額；若符合施行令第 48 條之 11 第 2 項任一款情形者，依其違法行為之重大性核算：違法行為相當重大者，核算金額為 3 億 6 千萬韓幣、違法行為重大者，核算金額為 2 億 8 千萬韓幣、違法行為通常者，核算金額為 2 億韓幣；另依前揭標準產生初步核算金額前，仍應考量對違法行為重大性之故意、有無重大過失、有無營利目的、受害規模、個人資料有無對公眾外流，及因違法行為獲取之利益範圍等綜合評估以計算核算金額。

其次，第二步驟：對該核算金額依情節認定有無加重、減輕之必要，係指經第一步驟之核算金額，應依違法行為之存續期間及次數等情節判斷核算金額有無加重、減輕之必要，於必要時以百分之五十範圍內為加重或減輕。

第三步驟：對該核算金額依情節認定是否為加重、減輕之補充，係就經第二步驟為必要加重、減輕之核算金額，應視對個人資料保護努力程度、有無配合違法行為調查、有無主導違法行為等為整體考量，得於百分之五十範圍內為補充加重或減輕。

最後，第四步驟：決定應裁罰之罰鍰，係指對違法行為人為裁罰前得依相當情節再次確認得減輕或免除裁罰；就得減輕部分，乃委員

會最終決定罰鍰前得考量違法行為人現實上負擔能力、違法行為發生後對個資當事人的侵害程度及賠償金額、違法行為人所屬產業或市場是否因經濟危機致顯著的變動或狀態持續惡化等，認經前三步驟核算金額過重時，得於該核算金額之百分之九十內為減輕，決定應裁罰之罰鍰。得免除裁罰部分，於符合違法行為人有給付不能、停止支付或資本虧損等事由認違法行為人客觀上無給付能力時、違法行為之內容及程度極其輕微、核算金額為小額、違法行為人有正當事由無法認知自己的行為違法時等任一情節時，委員會得免除裁罰。惟附表 1 之 5 僅係核算罰鍰的基本程序及方法，就相關銷售額、違法行為重大性、加重及減輕之必要、加重及減輕之補充等判斷標準，以保護委員會 2020 年 8 月 5 日制定公布之「（個人情報保護委員會）違反個人情報保護相關法規之課徵金課賦基準」⁵⁵（以下稱課賦基準）為參考依據。

(2) 參考基準

課賦基準具訓示性質，依該基準第 1 條內容可知本基準制定目的係為就個資法第 39 條之 15 第 3 項、個資法施行令第 48 條之 11 第 4 項及同施行另附表 1 之 5 等課賦罰鍰規定⁵⁶，予以具體之判斷基準。因此根據課賦基準各條文，委員會於核算裁罰額時，除依個資法第 39 條之 15 第 3 項各款事由審酌行為的影響外，及依附表 1 之 5 第二步驟核算金額外，就核算程序中應參考之與該違法行為相關、重大性判

⁵⁵ 原文為「(개인정보보호위원회) 개인정보보호 법규 위반에 대한 과징금 부과기준」。

⁵⁶ 見「（個人情報保護委員會）違反個人情報保護相關法規之過徵金課賦基準」第 1 條。

斷、必要之加重及減輕、計算違反期間⁵⁷、補充之加重及減輕等細節，得參考課賦基準之規定為判斷。

課賦基準第 4 條規定於決定「與該情報通信服務提供者之違法行為相關的情報通信服務前 3 個事業年度之年均銷售額」時，應依「電子通信事業法」第 5 條規定，並審酌提供服務之方式、加入服務之方法（例如線上加入抑或線下加入，以及倘若該公司有經營數個網頁，則得否個別加入各網頁等）、利用規約中規定之服務範圍，以及對管理個人資料之組織、人力及系統運行方式等情節，參考有關服務銷售額之會計資料決定「與違法行為相關銷售額」；倘若依前揭方式決定「與違法行為相關銷售額」有困難，則可透過該情報通信服務提供者過去的業績、同種勞務提供商之過去業績、事業計畫、以及市場現況等綜合評估後決定該「與違法行為相關銷售額」。

而在行為重大性的判斷上，依課賦基準第 5 條第 1 項規定，以違法行為是否為故意或重大過失、有無營利目的、有無執行施行令第 48 條之 2 規定之安全維護措施等為考量，如通信情報服務提供者對違法行為無重大過失時，其違法行為屬於通常程度、若對違法行為有故意或重大過失時，其違法行為屬於相當重大。惟當被視為「相當重大」之違法行為有未自違法行為中獲取直接利益、違法行為所致之受害規模僅占該情報通信服務提供者所有個人資料之百分之五，及利用人之個人情報未對公眾洩漏等任一酌減事由時，原相當重大得減為重大，

⁵⁷ 違反期間通常係以違法行為始日起至違法行為終止日為計算基準；惟當違法行為經委員會命令裁罰後仍繼續時，以委員會審議終止日視為違法行為終止日，因違反期間可能影響違法行為次數的計算，藉由課賦基準第 7 條第 1 項規定予以明確。另違法行為始日及終止日不明時，可參考違法行為人之營業及財務相關資料、員工及利用人之陳述，以及同類勞務供應商之營業及交易實際情形等計算之。

若情報通信服務提供者完全符合前揭酌減事由時，原相當重大以通常論。行為重大性經判斷後即可參考附表 1 之 5 第一步驟得出核算比率。

附表 1 之 5 第二步驟必要加重及減輕，其判斷依**違法行為之存續期間及違反次數之順序**為之。首先，違法行為之存續期間分為短、中、長期，存續期間以 1 年以內為短期，符合短期者無需加重核算金額，中期為 1 年以上未滿 2 年，需對核算金額加重百分之二十五、長期為 2 年以上，符合長期者應加重百分之五十，據此確認核算金額之必要加重後，再以違反次數確認必要減輕。違反次數以該情報通信服務提供者於最近三年間，有無因違法行為被依個資法第 39 條之 15 第 1 項科處罰鍰⁵⁸，若無則就經前揭必要加重判斷後核算金額於百分之五十內為必要減輕，若該情報通信服務提供者於最近三年間，有因違法行為被依個資法第 39 條之 15 第 1 項科處罰鍰 1 次以上即累犯，則無必要減輕之適用。

補充之加重及減輕係視對個人資料保護努力程度、有無配合違法行為調查、有無主導違法行為等為整體考量，得於百分之五十範圍內為補充加重或減輕，依課賦基準附表內容，分為加重比率及減輕比率。就加重比率部分，如委員會依個資法第 63 條第 1、2 項要求違法行為人提出相關物品及文件等資料時，違法行為人及其所屬員工有拒絕接受調查、湮滅證據、偽造虛假情報等方式妨害調查時，或相關利用人有虛假陳述時，則得於百分之三十內對核算金額為補充加重；另於多數業者有主導或誘使違法行為及相關情況產生，則得於百分之二十內對核算金額為補充加重。於補充減輕部分，若情報通信提供服務者就

⁵⁸ 是否曾被科處罰鍰之認定，應排除「糾正措施」之命令、經判決確定裁罰無效或撤銷等情節。詳見課賦基準第 6 條第 3 項規定。

個人資料保護取得委員會認證，得於百分之五十內對核算金額為補充減輕、積極配合委員會調查則得於百分之三十內對核算金額為補充減輕、主動通報個人資料外流事實者得於百分之三十內對核算金額為補充減輕。

此課賦基準係委員會為裁罰罰鍰前的參考標準，就如何判斷違法行為之重大性、何種情況得給予減輕及加重等均為更具體之細部規定。

4. 裁罰實務

(1) 委員會於 2022 年 12 月 14 日召開該年度第 20 次全體會議，以違反個資保護規定為由分別對 Gmarket、TRN、Wconcept 等三間公司祭出裁罰，罰鍰總額為韓幣 3 億 6,084 萬元，及行政罰款總額為 1,320 萬韓幣⁵⁹。

委員會於受理 Gmarket、TRN、Wconcept 等三間公司個人資料外流申告後即著手調查，調查結果認定有未盡安全維護措施義務，且未主動通報個人資料外流事實，經綜合評估各該公司的違法行為後予以裁處。

Gmarket 旗下 Auction 購物網站之顧客中心以電子郵件回覆客戶申訴時，誤將第三人的申訴內容併同回覆致該第三人的個人資料外流，因 Gmarket 於知悉個人資料外流事實之 24 小時內未為通報及通知，認違反個資法第 39 之 4 條第 1 項未即時通報及通知個資外流事實，裁處行政罰款（過怠料）360 萬韓幣。

⁵⁹ 新聞稿參考

<https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020000000&nttId=8357#LINK>（最後瀏覽日：2023 年 4 月 19 日）

TRN 網站之顧客中心在回覆用戶的疑問時，誤將包含該用戶個人資料之回覆內容設定為公開，導致客戶的個人資料外流，因 TRN 於知悉個人資料外流事實之 24 小時內未為通報，認違反個資法第 39 條之 4 第 1 項未即時通報個資外流事實，裁處行政罰款（過怠料）300 萬韓幣。

Wconcept 經營線上購物網站，該網站設有「贈送禮物」的功能，因禮物箱連結設定錯誤，致系統自動透過 Kakaotalk 傳送連結給受訊方時，有 2,583 筆個人資料外流，且 Wconcept 於知悉個人資料外流事實之 24 小時內未為通報及通知，認違反個資法第 29 條、第 39 條之 4 第 1 項，未盡安全措施義務、未即時通報及通知個資外流事實，裁處糾正命令、罰鍰 3 億 6,084 萬韓幣及行政罰款（過怠料）660 萬韓幣。

(2) 委員會於 2023 年 3 月 8 日召開該年度第 4 次全體會議並以違反個資保護規定為由分別對 SL Biotech、TNK Factory、KGedune、CheongDPK⁶⁰等四間公司祭出裁罰，罰鍰總額為 4 億 8,342 萬元，及行政罰款總額為 3,480 萬韓幣⁶¹。

SL Biotech、TNK Factory、KGedune、CheongDPK 等四間公司均經營線上網站提供服務，本次裁罰過程係委員會分別收到對此四間公司有個人資料外流事實的告發後，著手對此四間公司展開調查。調查結果確認四間公司均未盡安全維護措施義務，且未主動通報個人資

⁶⁰ 原為南韓達美樂公司，後更名。

⁶¹ 新聞稿參考

<https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020000000&nttId=8680>（最後瀏覽日：2023 年 4 月 19 日）

料外流事實及未為通知義務等情節，經綜合評估各該公司的違法行為後予以裁處。

SL Biotech 經營保健食品公司購物網站，因未於個人資料處理系統中設置存取權限制，使惡意文件可輕易上傳並執行，導致 75 名客戶的信用卡消費情報及 11 萬 9,756 名客戶的個人資料遭到外流，且 SL Biotech 對此外流事實亦遲誤通報及通知，認違反個人資料保護法第 29 條、第 39 條之 4 第 1 項，未盡安全措施義務、未即時通報及通知個資外流事實，故裁處韓幣 4 億 6,457 萬元罰鍰及韓幣 720 萬元行政罰款。

TNK Factory 為廣告企劃公司，其經營購物網站時，因未於個人資料處理系統中設置存取權限制，使惡意文件可輕易上傳並執行，導致 1 萬 6,702 名客戶的個人資料遭到外流，且 TNK Factory 未個別通知受害者，認違反個人資料保護法第 29 條、第 39 條之 4 第 1 項，未盡安全措施義務、未即時通知個資外流事實，故裁處韓幣 1,138 萬元罰鍰及韓幣 960 萬元行政罰款。

KGeduone 經營線上教育服務網站，其未依法律規定即處理 494 筆住民登錄號碼，且未設置目錄索引 (Directory Listing)⁶²關閉措施，導致有 1,136 筆身分證被揭露於搜尋引擎，KGeduone 延誤通報個資外流事實，認違反個人資料保護法第 24 條之 2 第 1 項、第 29 條、第 39 條之 4 第 1 項，違反住民登錄號碼處理限制、未盡安全措施義務、未即時通知個資外流事實等，故裁處韓幣 747 萬元罰鍰及韓幣 1,080 萬元行政罰款。

⁶² 指網站伺服器直接瀏覽目錄索引功能，若未關閉瀏覽目錄索引，可透過目錄索引檢視伺服器所存放的目錄及資料。

CheongDPK 經營外送披薩網站，未驗證電子郵件有效性，會員識別邏輯設定有誤，即以簡易認證方式加入之會員及一般基本會員，當兩者電子郵件一致時識別為同一會員，導致 1 名用戶個人資料外流，而 CheongDPK 就此外流延誤通報及通知，認違反個人資料保護法第 29 條、第 39 條之 4 第 1 項，未盡安全措施義務、未即時通報及通知個資外流事實，故裁處韓幣 720 萬元行政罰款。

前揭裁罰對象均經營線上網站，屬「情報通信服務提供者」，其等違法行為應優先適用個資法第 39 條之 15 規定；惟 Gmarket 及 TRN 兩家公司係違反個資法第 39 條之 4 第 1 項，同法第 39 條之 15 無違反第 39 條之 4 第 1 項應裁罰罰鍰之規定，故委員會依個資法第 75 條第 2 項第 12 款之 3 規定，以違反個資法第 39 條之 4 第 1 項對其等違法行為僅裁處行政罰款。而其他公司除違反第 39 條之 4 第 1 項通報及通知義務外，亦同時違反個資法第 29 條時，依個資法第 39 條之 15 第 1 項第 5 款明文規定情報通信服務提供者未依個資法第 29 條設置措施，得課賦「與該違法行為相關」銷售額百分之三以下之罰鍰，故委員會得對未盡安全措施義務之違法行為議決裁罰之罰鍰額。

（四）案例

1. 2020 헌바 (憲 BA) ⁶³259

⁶³ 依憲法裁判所受理案件相關規則第 8 條案件編號的組成之規定，헌바係代表該案件為第二種憲法訴願審判事件，即憲法裁判所法第 68 條第 2 項「違憲法律審查類型」之訴願案件。此處使用憲 BA 係「헌」代表憲，表示憲法裁判所的案件（如果是刑案則為「형」代表刑，以此類推）；而바是案件編號，依規則除代表第二種憲法訴願審判事件外，無其他意義，亦無其他漢字可以替代，因此採用音譯，以 BA 表示以避免混淆，此亦為韓文常見的音譯表示方法。

(1) 案由

情報通信網利用促進暨情報保護等相關法律第 64 條之 3 第 1 項
本文等違憲訴願

(2) 案件概要

網路商城 INTERPARK 在 2016 年 5 月 3 日至同年月 6 日間遭駭客入侵，經放送通信委員會（相當於我國國家通訊傳播委員會）以 INTERPARK 未於其個人資料處理系統完備如限制最長連接期間等控制存取裝置，亦未採取密碼管理等安全措施，致逾 2,540 萬筆個人資料對外流漏，認 INTERPARK 違反「情報通信網利用促進暨情報保護等相關法律」第 28 條第 1 項第 2 款、第 4 款等規定，依同法第 64 條、第 64 條之 3、第 76 條等規定發出改正命令，公布個資受侵害之事實、命 INTERPARK 應於施行教育及確立對策後提出報告，並裁罰 44 億 8,000 萬韓幣之罰鍰（課徵金）及 2,500 萬韓幣之行政罰款（過怠料）；INTERPARK 於受裁罰後即提出行政訴訟，主張除 2,500 萬韓幣行政罰款外，其餘裁罰及命令無效；此案經首爾行政法院、首爾高等法院駁回後，INTERPARK 向大法院提起上告⁶⁴，於大法院審理進行中復以「情報通信網法」第 64 條之 3 第 1 項第 6 款及同條第 2 項但書聲請提請違憲審判，大法院於 2020 年 3 月 12 日駁回其上告及聲請，INTERPARK（以下稱請求人）嗣於同年 4 月 17 日向憲法裁判所提起憲法訴願。

(3) 審查對象

⁶⁴ 南韓行政訴訟三審制，第一審為起訴（기소）、不服第一審判決向第二審提起抗訴（항소），故第二審又稱為抗訴審（항소심），不服第二審判決向第三審提起上告（상고），第三審又稱為上告審（상고심）。

本案以舊「情報通信網法」（2014.5.28. 法律第 12681 號, 2016. 3. 22. 法律第 14080 號）第 64 條之 3 第 1 項第 6 款規定中「情報通信服務提供者未設置第 28 條第 1 項第 2 款及第 4 款措施導致使用人之個人情報有外流情事時」（課徵金裁罰條款）及舊「情報通信網法」（2012. 2. 17. 法律第 11322 號, 2020. 2. 4. 法律第 16955 號修正前）第 64 條之 3 第 2 款但書（例外基準條款）等條文進行違憲審查。

(4) 本案爭點

- (a) 課徵金⁶⁵裁罰條款係「情報通信服務提供者」違反舊「情報通信網法」第 28 條第 1 項第 2 款及第 4 款規定，未設置安全措施致使用人的個人資料外流，課徵與違法行為相關銷售額百分之三以下之相當金額作為裁罰，此條文是否已限制「情報通信服務提供者」的營業自由，裁罰致財產減少是否侵害財產權。
- (b) 課徵金裁罰條款以「與違法行為相關營業額」為基準計算百分之三核定課徵金，則此「與違法行為相關營業額」之意義不明，有否違反明確性原則，而核定課徵金之基準是否有違禁止過度評價原則。
- (c) 另請求人雖以課徵金裁罰條款就違法行為與個人資料外流間不具因果關係，或情報通信服務提供者係善意無過失時仍裁處課徵金，主張此條文有違正當性原則、比例原則、更有請求權人基本權受侵害等等，惟此部分於判斷是否有違禁止過度評價原則即可併予審查，無需再另行判斷。

(5) 審查結果

⁶⁵ 為盡可能貼近判決原文，涉及判決內容以課徵金取代罰鍰。

「情報通信服務提供者」違反安全措施義務應裁處相關課徵金之規定，係 2008 年 6 月 13 日以明文規定於「情報通信網法」部分修正案（2008 年 12 月 14 日施行），此前就該違反義務行為已有過怠料（行政罰款）及刑事處罰等相關罰則，惟個人資料之盜用、洩漏等事件，通常非「情報通信服務提供者」為獲取利益而直接為之，絕大部分係「情報通信服務提供者」未設置安全措施等過失致第三方有機可趁而為侵害行為，因此課徵金裁罰條款之立法目的包含追繳與違法行為相關之不法利得、實現履行個人資料安全措施義務之行政願景，同時具備處罰違法行為及罰鍰等特性，與原有的過怠料及刑事處罰不同；基於前揭同時具備處罰違法行為及行政罰鍰等特性，課徵金裁罰條款之「與違法行為相關營業額」並非僅指涉「因違法行為所取得之利益」，更包括因違法行為直接或間接影響所獲取之銷售額。再者，新技術持續發展變化，設置保護措施難度降低，運用個人資料可獲取的利益範圍及侵害程度極廣，且網際網路的特性使個人資料外流的方式變化多端，難以區分未設置保護措施對個人資料外流所產生的影響係直接或間接，因此法律條款未具體規定「與違法行為相關」，而係立法技術上予以保留依個案適用，故課徵金裁罰條款之「與違法行為相關營業額」，經評估個人資料於當今社會可進行大量的經濟活動，可充分知悉該條款所指非僅限於違法行為所能直接獲取的利益，更包含違法行為直接或間接影響的服務銷售額，據此該條款無違反明確性原則。

隨著技術的發展，越來越多人利用情報通信服務，並將姓名、住民登錄號碼提供給情報通信服務提供者，使企業間所有之個人資料急劇增加，經常發生個人資料外流事件，並產生盜用姓名、偽造身分證、電話詐騙等 2 次侵害，而課徵金裁罰條款係為強化情報通信服務提供

者履行設置個人資料保護措施之義務，以防止個人資料外流而制定，此條款具有目的正當性，課賦課徵金亦能促使情報通信服務提供者履行設置個人資料保護措施之義務，認此條款具有手段適當性。

課徵金裁罰條款僅裁罰情報通信服務提供者未運行控制裝置，及未設置安全儲存或傳送個人資料之安全措施等法律明示阻斷不法存取行為之保護措施，即情報通信服務提供者已履行措施義務仍無法防止第三人引發個人資料外流時，無課徵金裁罰條款適用，因此課徵金裁罰條款其裁罰內容未逾越情報通信服務提供者之責任範圍；至課徵金裁罰條款立法目的不僅在於追繳不法利得，更有透過制裁抑制違法行為的意味，而依銷售額為基準雖可能導致課徵金極高的情形，但對於高銷售額的情報通信服務提供者而言，其可能蒐集及保存大量的個人資料，則考量受害範圍，對其制裁強度亦有提升之必要，況保護個人資料所設置之技術性、管理性措施，雖須投入相當費用，然此與因裁罰所生之經濟損失相比，設置保護措施之費用顯得微不足道，因此透過銷售額規模為裁罰基準，具有抑止違法行為之效果。而課徵金裁罰條款之「與違法行為相關營業額百分之三」，其最終裁罰額由放送通信委員會（判決依違法行為發生時而適用舊情報通信網法之規定）考量違法行為之內容及程度、違法行為存續期間及次數、因違法行為所獲取之利益規模等情節而定之，故仍係根據個案特性及違法程度依比例於相當金額範圍內課賦課徵金，可謂為達成課徵金裁罰條款立法目之必要基準，難謂有裁罰過重乙情，認此條款符合侵害最小化。

於法益衡平部分，雖然課徵金裁罰條款可能產生高額的裁罰額，惟考量個人資料外流可能發生二次侵害，如情報通信技術發達使大規模處理個人資料變得極為容易，線上金融交易活躍發展的同時，第三

人惡意利用個人資料的危險性亦提升等，則情報通信服務提供者未履行個人資料保護措施義務之制裁以防止個人資料外流之公益性，相較於情報通信服務提供者違法行為被裁罰之經濟上不利益，公益明顯大於私益，因此課徵金裁罰條款符合法益衡平原則。

綜上，課徵金裁罰條款符合禁止過度評價原則，未侵害請求人之營業自由及財產權，並為主文如下：

- (a) 舊「情報通信網法」（2012. 2. 17. 法律第 11322 號, 2020. 2. 4. 法律第 16955 號修正前）第 64 條之 3 第 2 款但書（例外基準條款）之審判請求駁回。
- (b) 舊「情報通信網法」（2014. 5. 28. 法律第 12681 號, 2016. 3. 22. 法律第 14080 號）第 64 條之 3 第 1 項第 6 款規定中「情報通信服務提供者未設置第 28 條第 1 項第 2 款及第 4 款措施導致使用人之個人情報有外流情事時」(課徵金裁罰條款)合憲。

二、簡析

現行南韓「個人情報保護法」第 6 章「情報通信服務提供者等之處理個人情報等特例」即第 39 條之 3 至第 39 條之 15，此章節乃為整合數據 3 法及貫徹個人資料一元化保護原則，遂於 2020 年修法時將過去「情報通信網法」的規定以近乎原封不動的方式併入「個人情報保護法」，因此該章節的裁罰主體為以營利為目的利用網路(通訊)服務提供資料或居間提供資料之人，即線上服務產業(internet/online company)；然而線上(視訊)社會的急速發展，線上服務產業及實體服務產業的界線變得模糊，現行法對實體服務產業及線上服務產業適用之裁罰規範不同，導致初次為違法行為之人應適用何裁罰規範或

是該給予雙重裁處等形成不同意見。對此，南韓個人情報保護委員會於 2021 年 1 月 6 日公布「個人情報保護法」的修正草案⁶⁶（以下稱 2021 修正案），刪除第 6 章「情報通信服務提供者等之處理個人情報等特例」，並以所有「個人情報處理者」的「同一行為—同一規範」⁶⁷為裁罰適用原則，新制定若干條文以因應現行法適用的難處，即「情報通信服務提供者」不再適用特例而回歸一般規定⁶⁸。

今年（2023 年）2 月 27 日南韓國會通過個資法修正案，並於同年 3 月 14 日公布，同年 9 月 15 日施行，行政罰鍰為部分修正，修正理由為侵害個人資料事件多係以獲取經濟上利益為目的，然現行法對這類型事件的裁罰仍以刑罰為中心，著重在處罰「人」，常被詬病實行效益過低，且現行法以違法行為相關之銷售額為基準計算課徵金時，如遇駭客入侵該如何排除無關的銷售額此類爭議往往成為進入訴訟的攻防重點，核定行政罰鍰（課徵金）爭議不斷，因此參考歐盟等海外先進國的立法例，以強化經濟罰為重點，認為確保企業事前的義務標準及責任，有必要對企業之違法行為課以相當的罰鍰（課徵金），故新制定第 64 條之 2 規定以因應現行法於經濟罰上的不足。

⁶⁶ 「개인정보 보호법」 일부개정법률(안) 입법예고 <https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS061&mCode=C010010000&nttId=7059#LINK>

（最後瀏覽日：2023 年 4 月 19 日）。

⁶⁷ 동일행위-동일규제.

⁶⁸ 個人情報保護委員會公布之「조문별 제개정이유서(개인정보보호법 일부개정법률안)(최종)」，來源為 <https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS061&mCode=C010010000&nttId=7059#LINK>

（最後瀏覽日：2023 年 4 月 19 日）。

新法第 64 條之 2 以現行法第 39 條之 15 為基礎，裁罰對象從「情報通信服務提供者」擴張適用於所有「個人資料處理者」，現行法第 28 條之 6 及第 34 條之 2 規定亦均併入本條文，條文內容如下：

第 64 條之 2（課賦課徵金）

1. 個人情報處理者有下列各款之任一行為時，保護委員會得於不超過整體銷售額百分之三範圍內課賦課徵金。但無銷售總額或計算上顯有困難時，得依大統領令規定，於不超過韓幣 20 億元之範圍內課賦之。
 - (1) 違反第 15 條第 1 項、第 17 條第 1 項、第 18 條第 1 項及第 2 項（包含依第 26 條第 8 項準用規定），或第 19 條等處理個人情報時；
 - (2) 違反第 22 條第 1 項（包含依第 26 條第 8 項準用規定）未取得法定代理人同意而處理 14 歲以下兒童之個人情報時；
 - (3) 違反第 23 條第 1 項第 1 款（包含依第 26 條第 8 項準用規定）未取得情報當事人同意即蒐集敏感情報時；
 - (4) 違反第 24 條第 1 項、第 24 條之 2 第 1 項（包含依第 26 條第 8 項準用規定）處理固有識別情報或住民登錄號碼時；
 - (5) 疏於進行第 26 條第 4 項規定之管理、監督或教育致受託者有違反本法規定時；
 - (6) 違反第 28 條之 8 第 1 項（包含依第 26 條第 8 項準用規定）以識別特定個人為目的而處理情報時；
 - (7) 違反第 28 條之 8 第 1 項（包含依第 26 條第 8 項及第 28 條之 11 之準用規定）移轉個人情報至國外時；

- (8) 違反第 28 條之 9 第 1 項（包含依第 26 條第 8 項及第 28 條之 11 之準用規定）未遵循國外移轉終止命令時；
- (9) 個人資料處理者處理個人情報有遺失、竊取、洩漏、偽造、變造及毀損時。但個人情報處理者有依第 29 條（包含依第 26 條第 8 項準用規定）設置安全維護必要措施以防範個人情報有遺失、竊取、洩漏、偽造、變造及毀損時，不在此限。
- 2. 保護委員會欲依第 1 項規定課賦課徵金時，應以整體銷售額排除與違法行為無關之銷售額後為基準，算定課徵金。
- 3. 保護委員會欲依第 1 項規定課賦課徵金時，個人情報處理者無正當事由而拒絕提供核算銷售額資料或提出虛假資料時，以該個人情報處理者整體銷售額為基準核算之，並依與該個人資料處理者相似規模之個人情報處理者，其個人情報保有程度、財務報表等會計資料、商品或勞務之價格等營業現況為根據，推定其銷售額。
- 4. 保護委員會依第 1 項課賦課徵金時，應評估下列各款事項以兼顧違法行為及預防侵害間之比例及效果：
 - (1) 違法行為之內容暨程度；
 - (2) 違法行為之期間暨次數；
 - (3) 依違法行為而取得利益之規模；
 - (4) 致力於執行加密化等安全性維護措施；
 - (5) 個人情報遺失、竊取、洩漏、偽造、變造及毀損等情形與違法行為之關聯性及失、竊取、洩漏、偽造、變造及毀損等之規模；

- (6) 有無回復違法行為所致之侵害，及有無執行預防侵害擴散之措施；
 - (7) 個人情報處理者之業務現況及規模；
 - (8) 個人情報處理者處理之個人情報類型及對情報當事人之影響；
 - (9) 情報當事人因違法行為所致之受害程度；
 - (10) 致力於保護個人情報而有個人情報保護認證、自發性保護行為等；
 - (11) 有無配合保護委員會進行相關措施以改正違法行為；
5. 有符合下列任一款事由之情形，保護委員會得不課賦課徵金：
- (1) 有給付不能、停止支付或資本虧損等事由，客觀上認無給付能力時；
 - (2) 有正當事由無法認知自身行為違法；
 - (3) 違法行為之內容或程度極其輕微、核算金額為小額時；
 - (4) 其他對情報當事人未生侵害或依大統領令所定具備極輕微事由時；
6. 第 1 項課徵金經第 2 項至第 5 項評估後核定，具體之核定基準與核定程序以大統領令定之。
7. 根據第 1 項應繳納課徵金而未於繳交期間內繳納者，保護委員會應加徵自繳納期間屆滿次日起算課徵金之百分之六年利率之滯納金。據此滯納金之徵收期間不得超過 60 個月。
8. 根據第 1 項應繳納課徵金者有未於繳交期間內繳納之情形，保護委員會應定期限催繳，如於該指定期限內仍未繳納課徵金及第 7 項之滯納金，則依國稅滯納處分先例徵收。

9. 有法院判決等事由而需返還第 1 項所課賦之課徵金時，自繳納課徵金之日起至返還日止之期間內，應評估金融公司之存款利率等，適用大統領令所定之利率核算返還滯納金並給付。
10. 除第 9 項規定外，依法院判決取消該課賦課徵金處分，而判決理由中有課賦新的課徵金時，保護委員會以當初已繳納之課徵金扣抵新的過徵金，並僅就剩餘返還課徵金額計算返還滯納金併予返還。

新法將現行法第 39 條之 15 對違法行為課賦罰鍰（課徵金）上限「與違法行為相關銷售額百分之三以下之課徵金」，提升為「整體銷售額的百分之三」，即行政罰鍰上限不再區分銷售額是否跟違法行為有關；惟新法第 2 項亦規定算定課徵金仍須以整體銷售額中扣除與違法行為無關之銷售額後之剩餘銷售額為基準，似保留現行法「與違法行為相關銷售額」之規定，此與 2021 年 1 月 6 日初次公布之修正草案中不再區分「與違法行為相關銷售額」，均以「整體銷售額的百分之三」為罰鍰上限略有不同，當時的修正理由是為因應國際趨勢及避免計算罰鍰時產生爭議，而對該草案反對意見認為在無法確認母公司在國外的外國企業之「整體銷售額」，此修正似僅加重本國企業的裁罰責任，將生差別上爭議，因此國會對修正案進行審議時，就此條文為適度的調整。

南韓個資人權團體批評此調整猶如「朝三暮四」，認為相較於 GDPR 以年度銷售額百分之四作為裁罰基準，調整後的新法對個資保護顯然在走回頭路；對此保護委員會委員長於今年 3 月 7 日就新法內容為說明時回應認 GDPR 雖然重要，但難以將其視為「國際標準」，且現行法「與違法行為相關」之舉證責任在保護委員會，而新法係將「與違法行為相關銷售額之舉證責任」轉換由企業負擔，當企業無法

提出相關證明資料或偽造資料時，則得依「整體銷售額的百分之三」課賦罰鍰，不能輕忽此規範抑制違法行為之效果⁶⁹，雖被認為朝三暮四，但此修法得有效減輕委員會的業務負擔⁷⁰。

新法預計於今年 9 月 15 日施行，修正後的行政裁罰與個人資料保護間的衡平及影響，其實際適用情況仍需待施行後予以觀察。

⁶⁹ 「개인정보 보호·활용 포지티브섬 게임

돼야」新聞網址：<https://shindonga.donga.com/3/all/13/4047763/1>（最後瀏覽日：2023 年 4 月 19 日）

⁷⁰ 개정 개인정보법 과징금 ‘조삼모사’ 논란에...담당부처 답변은?

新聞網址：<https://www.hani.co.kr/arti/economy/it/1082532.html>（最後瀏覽日：2023 年 4 月 19 日）

第四章 針對我國之建議

第一節 我國法制中的雙規制裁罰上限

與歐盟類似，我國競爭法制中，針對行政罰鍰之上限，亦設有固定—浮動雙軌制裁罰上限。依公平交易法第 40 條第 1 項和第 2 項，事業如違反該法第 9 條或第 15 條之規定，主管機關公平交易委員會（下稱公平會）得限期令停止、改正其行為或採取必要更正措施，並得處新臺幣十萬元以上五千萬元以下罰鍰；如該事業屆期未遵守公平會命令，得按次處新臺幣二十萬元以上一億元以下罰鍰。然如公平會認定事業違法行為情節重大，得處該事業上一會計年度銷售金額百分之十以下罰鍰，不受前述罰鍰金額限制。

公平會並依公平交易法第 40 條第 3 項授權，訂定事業上一會計年度銷售金額之計算、情節重大之認定、罰鍰計算之辦法，即《違反公平交易法第九條及第十五條情節重大案件之裁處罰鍰計算辦法》（以下稱公平會罰鍰辦法）。下文將分析公平交易法及該辦法之規範內容，以及公平會於實務中對該規範之適用。

一、公平會規範重點

（一）浮動上限之適用範圍

綜合公平交易法第 40 條及公平會罰鍰辦法之規定，浮動上限之適用須同時滿足三項條件：違法行為之內容，違法行為之嚴重性，以及違法事業之銷售額規模。

1. 違法行為之內容

依公平交易法第 40 條第 2 項，浮動上限僅適用於違反該法之獨占行為與聯合行為。依其立法理由，此類違法行為之不法獲利通常較

高，為避免罰鍰金額與不法獲利顯不相當，確實遏制違法，故增訂浮動上限規範。由此觀之，我國公平交易法導入浮動上限制度，主要目的在於剝奪違法行為之違法所得，並落實對違法行為之懲戒性。

- (1) 第 9 條關於獨占事業禁止行為之規定，包括：以不公平之方法，直接或間接阻礙他事業參與競爭；對商品價格或服務報酬，為不當之決定、維持或變更；無正當理由，使交易相對人給予特別優惠；其他濫用市場地位之行為。
- (2) 第 15 條聯合行為禁止之規定：除有第 15 條但書所列情形之一，而有益於整體經濟與公共利益，且經申請主管機關許可外，事業不得為聯合行為。

2. 違法行為之嚴重性

依公平交易法第 40 條第 2 項，浮動上限僅適用「經主管機關認定情節重大」之違法行為。

依公平會罰鍰辦法第 2 條，違法行為「情節重大」，係指該行為嚴重影響市場競爭秩序，其認定應審酌下列事項：

- (1) 違法行為影響競爭秩序之範圍及程度。
- (2) 違法行為危害競爭秩序之持續時間。
- (3) 違法事業之市場地位及所屬市場結構。
- (4) 違法行為於違法期間之銷售金額及違法所得利益。
- (5) 違法行為類型為共同決定商品或服務之價格，或限制數量、交易對象、交易地區等聯合行為。

此外，公平會罰鍰辦法考量違法行為對市場競爭之影響，通常與違法所得、違法期間之銷售額成正相關⁷¹，故明定違法行為如達下列標準，得直接認為構成「情節重大」。

- (1) 獨占事業或參與聯合行為之一事業，其違法行為於違法期間內所獲商品或服務銷售金額逾新臺幣一億元。
- (2) 違法行為所得利益逾本法第四十條第一項所定罰鍰金額之上限。

3. 違法事業之銷售額規模

公平交易法第 40 條第 2 項規定，事業之違法行為經認定情節重大，則罰鍰金額得處該事業上一會計年度銷售金額 10% 以下罰鍰，「不受第 1 項罰鍰金額限制」。由此可見，公平交易法設置浮動上限之目的，係突破固定罰鍰上限。僅有當違法事業銷售額之 10% 超出固定罰鍰上限時（首次裁罰為五千萬元，未遵循公平會命令時每次一億元），才有浮動上限之適用。

（二）罰鍰之計算方式

1. 計算基本數額

依公平會罰鍰辦法第 5 條，「基本數額」係指違法行為於違法期間內所獲商品或服務銷售金額之百分之三十。

⁷¹ 違反公平交易法第十條及第十四條情節重大案件之裁處罰鍰計算辦法，立法理由，第 2 條，<https://www.ftc.gov.tw/upload/ca8b4b8a-c9f9-4ce0-b7f3-40cb2971db87.pdf>。

因此，公平交易法係將違法行為所獲收益之固定比例作為基本數額。主管機關在調查確認違法行為之相關事實後，如衡酌違法行為之影響、持續期間、銷售金額、所獲利益等因素，認定屬「情節重大」，即可直接依據違法期間之銷售金額，計算得出罰鍰之基本數額。

2. 依調整因素調整數額

依公平會罰鍰辦法第 6 條，主管機關對於計算得出之基本數額，得依據調整因素（加重或減輕事由）加以增減，以決定罰鍰額度。

其中，加重事由包括：

- (1) 主導或教唆違法行為。
- (2) 為確保聯合行為之遵守或履行而實施監督及執行制裁措施。
- (3) 五年內曾違反本法第九條或第十五條規定遭處分。

減輕事由包括：

- (1) 於主管機關進行調查時，立即停止違法行為。
- (2) 具懺悔實據，並配合調查。
- (3) 與受害者達成損害賠償之協議或已為損害之補救措施。
- (4) 因被迫而參與聯合行為。
- (5) 因其他機關之核准或鼓勵，或依法規之規定。

3. 確認罰鍰金額不得超過法定上限

依公平會罰鍰辦法第 7 條和第 3 條，主管機關對基本數額依加重或減輕因素予以調整後，所得出之罰鍰額度，不得超過受處分事業上一會計年度銷售金額之 10%。而事業上一會計年度銷售金額，指主管

機關「作成處分時」，該事業上一會計年度之營業收入總額。依第 3 條之立法理由，以「作成處分時」為依據，係為考量科處裁罰時，「違法事業之經濟實力及承受罰鍰之能力」；且「違法事業」之範圍，係以法人地位為基準，包括分公司在內，而不包括具有獨立法人格之子公司。

二、實務運作案例

104 年 12 月，公平會以違法實施聯合行為，足以影響我國鉭質電容器市場之供需功能且情節重大為由，採上一年度銷售額之 10% 為基準，對日商 NEC TOKIN Corporation（以下稱 Tokin）科處新臺幣 12 億 1,820 萬元罰鍰⁷²（系爭處分一），依公平會罰鍰辦法第 4 條之計算方式，對 Matsuo Electric Co.,Ltd.（以下稱 Matsuo）科處 2,430 萬元罰鍰⁷³（系爭處分二）。Tokin 和 Matsuo 不服系爭處分決定，分別提起行政訴訟。經臺北高等行政法院一審判決撤銷被訴之兩項系爭處分⁷⁴後，公平會提起上訴。

108 年 12 月，最高行政法院作出終審判決，就公平會系爭處分對違法行為之認定部分，廢棄高等行政法院之一審判決，並分別駁回 Tokin 和 Matsuo 之起訴，但在公平會之罰鍰金額計算部分，認為系爭處分一、系爭處分二分別存在計算違誤與裁量瑕疵，而維持一審判決，駁回公平會之上訴。

⁷² 公平交易委員會公處字第 104139 號處分書。

⁷³ 公平交易委員會公處字第 104140 號處分書。

⁷⁴ 臺北高等行政法院 105 年度訴字第 250 號判決、臺北高等行政法院 105 年度訴字第 284 號判決。

系爭處分一部分，最高法院認為，依 Tokin 行為時之公平會罰鍰辦法第 3 條及第 7 條規定，公平會應以 104 年 12 月 16 日作成處分時，Token 上一會計年度即 103 年之營業收入總額為計算基準，且不得將子公司之銷售金額納入計算。但公平會係依被 Token 102 年合併財務報表為據，將其全球各地子公司銷售金額納入計算，而有違誤⁷⁵。

系爭處分二部分，最高法院認為，公平會認定 Matsuo 違法期間為 94 年 4 月至 103 年 1 月止。Matsuo 雖已於該案調查期間，向公平會陳報其 94 年至 103 年鉅質電容器在臺灣銷售金額，然公平會認為會計或稅務資料多有保存年限，故採用實際所能獲得之最適當數據作為罰鍰之計算基礎，以 Matsuo 於 102 年售予臺灣的鉅質電容器銷售金額，乘以違法期間 8 年 10 個月所得金額之 30%，採計作為罰鍰基本數額。此不僅計算方法有違誤，且高估罰鍰基本數額，明顯不利於 Matsuo，亦有裁量濫用之違法。

最高法院作出前述判決後，公平會於 110 年 7 月分別針對罰鍰金額重為處分，在維持原處分情節嚴重性及加重減輕事由衡酌方式之前提下，重新計算罰鍰之計算基礎，將對 Token 之罰鍰降為新臺幣 11 億 4,522 萬元，將對 Matsuo 之罰鍰降為新臺幣 1,589 萬元。

第二節 比較分析

一、雙軌裁罰制度之整體設計

就雙軌裁罰制度之整體設計而言，歐盟和新加坡的裁罰制度較為相似，皆係以固定罰鍰金額上限為原則，針對年營業額達一定水準之

⁷⁵ 最高行政法院 108 年度判字第 597 號判決。

事業，則可突破固定上限，依事業年營業額計算浮動上限，以確保罰鍰之有效性與嚇阻性。相較之下，南韓 PIPA 則以浮動上限為原則，當個人情報處理者無銷售額或難以計算銷售額時，方可例外採用固定上限。我國公平交易法則明定「經主管機關認定違法情節重大」之行為，方可適用浮動上限，在某種意義上是將比例原則之要求明文化。對前述各國雙軌裁罰制度設計之細部比較如下。

（一）雙軌制之罰鍰金額

1. 雙軌制上限之規範模式

雙軌制上限之規範模式方面，歐盟和新加坡係以固定罰鍰金額上限為原則，於行為人之年營業額達較高水準時，以浮動上限為輔助，以利確保裁罰之有效性與嚇阻性。兩國（地區）並皆針對違反規範之種類，訂定不同上限。具體而言，歐盟以個資保護原則、個資運用之適法性、個資當事人權利行使、個資境外傳輸、遵守主管機關命令之規範為一類（第 83 條第 5 項、第 6 項），訂定 2000 萬歐元之固定上限、前一年度全球營業額 4% 之浮動上限；以個資安全維護、事故通知與通報、個資委外監督等為另一類（第 83 條第 4 項），訂定 1000 萬歐元之固定上限、前一年度全球營業額 2% 之浮動上限。新加坡則以個資蒐集與利用之適法性、個資當事人權利行使、個資境外傳輸、事故通知與通報等個資保護相關規範為一類，訂定 100 萬新加坡幣之固定上限、前一年度新加坡境內營業額 10% 之浮動上限；以謝絕聯絡規範為另一類，訂定個人 20 萬新加坡幣、其他人員 100 萬新加坡幣之固定上限，以及前一年度新加坡境內營業額 5% 之浮動上限。

南韓的模式則與其他兩國相反，以浮動上限為原則，於難以計算浮動上限時，例外適用固定上限。2020 年 PIPA 針對特定行為人或特定違法行為，局部採用雙軌制，其浮動上限之計算基礎不同（假名情報之違法行為：年均整體銷售額之 3%，情報通信服務提供者之違法行為：年均相關銷售額之 3%），然固定上限金額一致（皆為 4 億韓幣）。2023 年修正案在整合不同行為人之裁罰規範之同時，亦將不同違法行為之裁罰上限調為一致，皆以整體銷售額之 3% 為浮動上限，以 20 億韓幣為固定上限，而未針對違反不同規範作進一步區分。

我國公平交易法之罰鍰金額上限與歐盟、新加坡模式類似，亦以固定罰鍰金額上限為原則，以浮動上限為輔助，然並未根據違反之規範區分不同上限，而是針對拒不遵循主管機關改正命令之行為，規定較高之按次處罰上限。這或可認為是由於公平交易法僅局部採行雙軌制之故。綜合觀察公平交易法第 39、40、42、44 條之規定可知，該法整體仍是針對違反不同規範，規定不同罰鍰金額上限。

2. 罰鍰金額上限

罰鍰上限之具體金額方面，本研究所涉之先進國家個資法，其裁罰額度皆遠超我國現行個資法。依我國個資法第 47 條、第 48 條，對於違反個資蒐集處理利用適法性規範之行為，罰鍰上限為 50 萬元，對於違反當事人權利行使或個資安全維護規範之行為，罰鍰上限為 20 萬元。雖依行政罰法第 18 條第 2 項，法定罰鍰最高額得依個案中違反行政法上義務所得之利益而酌量加重⁷⁶，然而，除直接販售個資等

⁷⁶ 行政罰法第 18 條第 1 項規定，「裁處罰鍰，應審酌違反行政法上義務行為應受責難程度、所生影響及因違反行政法上義務所得之利益，並得考量受處罰者

情形外，違反個資法之行為通常難以直接產生經濟利益。例如，個資安全維護措施缺失是實務上常見違法行為，然對於因此所導致之個資侵害事故，蒐集機關往往自身也是受害者，而從無因此獲得收益。縱認為蒐集機關因降低安全水準而節約安全維護成本，因個資法對個資安全維護費用並無明確要求，亦難以確認蒐集機關因此節約之費用金額。因此，實務中，主管機關將難以適用行政罰法第 18 條第 2 項，突破個資法行政罰鍰之法定上限。

歐盟對違反第 83 條第 4 項所列規範之行為，雖設定較低之固定罰鍰金額上限 1000 萬歐元，折合新台幣超過 3 億元；對於對違反第 83 條第 5 項、第 6 項之行為，固定上限 2000 萬歐元，折合新台幣超過 6 億元。新加坡對組織違反個資保護規範之行為，罰鍰上限 100 萬新加坡幣，折合新台幣接近 2300 萬元，個人違反謝絕來電規範之罰鍰上限較低，為 20 萬新加坡幣，折合新台幣超過 450 萬元。南韓 2020 PIPA 雖以浮動上限為原則，罰鍰上限將視違法行為人之整體/相關銷售額而定，然因其適用範圍係以情報通信服務業者為主（其範圍包括網路服務提供者），故實際計算得出之罰鍰上限通常較高，實務中科處之罰鍰金額，也往往超出我國最高 50 萬元之上限；而對於無銷售額或難以計算銷售額之情形，則以 4 億韓幣為上限，折合新台幣接近 950 萬元。

就以上各國（地區）對事業之「最低」固定上限而言，歐盟為 1000 萬歐元，約為我國個資法「最高」罰鍰上限 50 萬元之 600 倍，新加坡為 100 萬新加坡幣，約為我國「最高」罰鍰之 50 倍，南韓為 4 億韓幣，約為我國「最高」罰鍰之 20 倍。

之資力」；第 2 項規定，「前項所得之利益超過法定罰鍰最高額者，得於所得利益之範圍內酌量加重，不受法定罰鍰最高額之限制」。

如以同類違法行為之裁罰上限觀察，我國與先進國家之落差將更為明顯。例如，若網路服務業者違反個資安全維護義務、侵害事故通知通報等義務，屬我國個資法第 48 條所列違法情事，罰鍰上限為 20 萬元⁷⁷。而同樣違反情事，依歐盟 GDPR 適用第 83 條第 4 項之罰鍰上限，在不考慮年營業額之前提下，裁罰上限為 1000 萬歐元，約為我國的 1500 倍；在新加坡屬違反第 6 章或第 6A 章之個資保護規範，在不考慮年營業額之前提下，罰鍰上限為 100 萬新加坡幣，約為我國的 125 倍。歐盟或新加坡以浮動上限為輔，若業者之年營業額達一定水準，則罰鍰上限可進一步提高。在南韓屬第 39-15 條之適用範圍，縱認該業者無相關銷售額，裁罰上限為 4 億韓幣，約為我國的 50 倍。

我國公平交易法雖因規範目的不同，而對個資法裁罰上限金額之參考性較低，然其罰鍰上限之設定，可協助評估我國產業與社會對行政罰鍰之接受程度。公平交易法於民國 88 年修法時，將行政罰鍰上限由 100 萬元提高至 5000 萬元，並進而於 101 年修法時，導入浮動

⁷⁷ 本研究係以 105 年施行之個資法為研析對象。本研究報告撰寫完成後，立法院於 112 年 5 月 16 日三讀通過個資法第 48 條修正案，經總統 112 年 5 月 31 日華總一經字第 11200045441 號令公布修正，自 112 年 6 月 2 日起生效，針對「違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法」之罰則，刪除原個資法第 48 條第 4 款，並增訂第 48 條第 2 項、第 3 項。經修正後之罰則不僅提高罰鍰上限至最高 1500 萬元，並刪除「先行命令改正」之要求，主管機關得針對違法行為，逕行裁處罰鍰。修正後之罰則如下：「由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣二萬元以上二百萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處新臺幣十五萬元以上一千五百萬元以下罰鍰。（第 2 項）非公務機關違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法，其情節重大者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣十五萬元以上一千五百萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處罰。（第 3 項）」。

上限制度。因此，如我國考量違反個資法行為對人民權利之侵害風險，為確保個資法規範之有效落實，擬修法上調罰鍰額度並導入浮動上限制度，公平交易法之修法經驗應可供參考。

3. 罰鍰金額下限

罰鍰金額下限方面，本研究所涉之先進國家個資法之行政罰鍰規範，皆未規定罰鍰金額下限，以提供主管機關依個案情形決定適當罰鍰額度之空間。且主管機關在實務中，亦不乏對非營利組織、個人等科處低額罰鍰之案例。例如，愛爾蘭 DPC 曾針對慈善團體個資安全維護措施不足之行為，裁處 1500 歐元（約合新台幣 5 萬元）罰鍰⁷⁸；比利時個資保護主管機關曾針對非營利組織違法利用個資行銷之行為，裁處 1000 歐元（約合新台幣 3.3 萬元）罰鍰⁷⁹。

與前述法律不同，我國個資法訂有罰鍰金額下限，且第 47 條規定，「非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之：……」。因此，如主管機關認定行為人確有該條所列之違法行為，則應科處罰鍰並命令改正。又因該條規定之罰鍰法定最高金額為 50 萬元，故縱個案違反情節輕微，

⁷⁸ Irish DPC, Decision in the matter of MOVE Ireland, DPC Case Reference: IN-20-7-1 (20 August 2021), <https://www.dataprotection.ie/sites/default/files/uploads/2021-11/IN-20-7-1%20Move%20Irl%20Final%20Decision.pdf>.

⁷⁹ Gegevensbeschermingsautoriteit, DOS-2019-04191 (mei 2020), <https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-28-2020.pdf>.

主管機關亦無依行政罰法第 19 條第 1 項⁸⁰職權決定免予處罰之裁量空間。

就我國立法習慣而言，以同時規定罰鍰上限與下限之方式居多，本研究所涉之公平交易法，亦對罰鍰訂有下限。然在允許主管機關較大裁量空間之法律中，亦有採用僅規定罰鍰上限、不規定罰鍰下限之方式⁸¹。因個資法裁罰規定適用於包括自然人在內之各類非公務機關，個案中違反情事可能顯著輕微、行為人較無資力，如我國擬修正個資法之罰則，似可考量放寬或移除罰鍰下限規範，或授權主管機關於個案中裁量減輕或免予處罰，以利確保個案罰鍰之合比例性。

（二）雙軌制罰鍰之適用

1. 罰鍰於執法措施中之定位

本研究所涉之先進國家個資法之罰鍰規範，皆將行政罰鍰與命令糾正列作主管機關行政執法權力，且允許主管機關裁量選擇是否單處或併處罰鍰或糾正措施。我國公平交易法第 40 條亦採類似模式，主管機關公平會針對違法行為，得裁量決定限期命令行為人停止、改正其行為或採取必要更正措施，和（或）裁處罰鍰。

⁸⁰ 行政罰法第 19 條第 1 項規定：「違反行政法上義務應受法定最高額新臺幣三千元以下罰鍰之處罰，其情節輕微，認以不處罰為適當者，得免予處罰」。

⁸¹ 例如，海關緝私條例第 37 條規定，「報運貨物進口而有下列情事之一者，得視情節輕重，處所漏進口稅額五倍以下之罰鍰，或沒入或併沒入其貨物：一、虛報所運貨物之名稱、數量或重量。二、虛報所運貨物之品質、價值或規格。三、繳驗偽造、變造或不實之發票或憑證。四、其他違法行為（第 1 項）。報運貨物出口，有前項各款情事之一者，處新臺幣三百萬元以下罰鍰，並得沒入其貨物（第 2 項）」。同法第 45-1 條規定，「依本條例規定應處罰鍰之行為，其情節輕微者，得減輕或免予處罰」。

相較之下，我國個資法依不同違法行為，規定不同裁罰措施。對於第 47 條所列違法行為（違反個資法第 6 條第 1 項、第 19 條、第 20 條第 1 項，或主管機關依第 21 條所為之限制個資國際傳輸之命令或處分），主管機關應命令改正並科處罰鍰，且得依個資法第 25 條作出禁止蒐集處理利用個資、沒入違法蒐集之個資、公布違法情形等命令或處分。對於第 48 條所列違法行為（違反個資法第 8 條至第 13 條、第 20 條第 2 項或第 3 項，或第 27 條⁸²），則須先行命令改正（得並處第 25 條所列命令或處分），行為人居期未改正，方可裁處罰鍰。

我國個資法現行規範模式，可能導致主管機關執法措施之有效性及嚇阻性不足。例如，業者個資安全維護措施不足、個資外洩事件頻發是我國社會當前面臨之重點問題。然因安全維護係個資法第 27 條規定事項、外洩事件通知當事人是第 12 條規定事項，業者違反此兩項規定，主管機關因個資法第 48 條規定限制，縱個案違反情節嚴重或影響重大，仍無權直接科處罰鍰，僅能先命令糾正，以致違法行為嚴重性與其裁罰措施顯然失衡⁸³。不僅不符社會通念下人民之期待，亦將阻礙個資法規範之充分落實，進而損及當事人權利之整體保護水準。

⁸² 本研究係以 105 年施行之個資法為研析對象。本研究報告撰寫完成後，立法院於 112 年 5 月 16 日三讀通過個資法第 48 條修正案，經總統 112 年 5 月 31 日公布修正，自 112 年 6 月 2 日起生效，明定違反個資法第 27 條之行為，主管機關得逕處罰鍰，不以先行限期改正為必要，詳如前註 77 所示。

⁸³ 同前註，本研究係以 105 年施行之個資法為研析對象。本研究報告撰寫完成後，立法院於 112 年 5 月 16 日三讀通過個資法第 48 條修正案，經總統 112 年 5 月 31 日公布修正，自 112 年 6 月 2 日起生效，明定違反個資法第 27 條之行為，主管機關得逕處罰鍰，不以先行限期改正為必要。

2. 違法行為人及行為樣態

違法行為人及行為樣態方面，歐盟和新加坡可謂全面採用雙軌裁罰制度，個資保護法律之各類適用對象（歐盟法中的控管者、受託運用者、認證機構與監督機構，新加坡法中的組織和人員）所實施之各類違法行為，包括個資蒐集處理與利用適法性、當事人權利行使、個資安全維護、事故通知與通報、個資境外傳輸等，皆設有雙軌裁罰。

相較之下，南韓 2020 年 PIPA 和我國公平交易法則屬局部性採用雙軌裁罰制度，適用範圍僅限於特定行為人（例如南韓法中的情報通信服務提供者、我國法中的獨占事業），或特定行為（例如南韓法中的利用假名情報識別當事人、我國法中的聯合行為）。

新加坡是 2020 年修法後，導入全面性雙軌裁罰制度。南韓 2023 年修正案則趨向於全面採行雙軌裁罰，在裁處課徵金時，原則上各類個人情報處理者之各類違反個資法行為，皆以雙軌制定其裁罰上限。由此可見，以雙軌裁罰制度協助確保裁罰之有效性和嚇阻性，提供主管機關行使行政執法權之彈性，已呈現增多趨勢。

此外，本研究所涉之先進國家個資法，皆在不同程度上對公務機關之裁罰設有例外規範。其中，新加坡 PDPA 第 4 條將公務機關排除於該法個資保護規範之適用範圍外，公務機關自不致因違反個資保護規範而遭 PDPC 裁罰。歐盟 GDPR 則允許會員國針對公務機關或機構之罰鍰另定規範。此與我國個資法執法措施以非公務機關為對象之現狀相一致。

二、罰鍰之計算方法

（一）計算步驟

就整體方法論而言，歐盟、新加坡和南韓法下，違反個資法之行政罰鍰計算步驟皆包括三個基本步驟：其一，依違法行為之嚴重性，確定罰鍰基本金額；其二，依加重或減輕事由，酌調罰鍰金額；其三，評估酌調後罰鍰金額之合比例性、有效性、嚇阻性及法定罰鍰上限限制，確定最終罰鍰金額。

實務執行中，三個國家（地區）之計算步驟各具特色。歐盟 EDPB 指引強調罰鍰之金額與違法行為人之規模（營業額）相當，故在確定罰鍰基本金額階段，即允許主管機關考量行為人之營業額，酌調裁罰基數。或許是為了調和各會員國主管機關之罰鍰計算方法，EDPB 指引著重量化各步驟之產出結果。南韓採浮動上限為原則之模式，罰鍰金額之計算自始即與行為人之整體/相關銷售額為基礎。南韓亦透過訂定罰鍰參考基準，量化罰鍰計算方式，以提升罰鍰金額之可預見性。新加坡修法之目的在於提供 PDPC 更多裁量空間，PDPC 於其指引和裁罰決定中，側重於定性描述罰鍰金額之計算步驟及衡酌要素。

我國公平交易法第 40 條對浮動上限罰鍰之計算步驟，遵循基本相同之模式，然有兩點不同：違法情節之嚴重性，係作為能否適用浮動罰鍰上限之前提條件；且違法行為人之年銷售額，僅作為確定罰鍰上限之考量要素，而未納入罰鍰基本金額或加重減輕之考量。

（二）罰鍰金額之計算基礎

1. 罰鍰基本金額

計算罰鍰基本金額時，歐盟與南韓 2020 年 PIPA 之方法類似，皆以法定罰鍰上限之「一定比例」作為罰鍰基本金額，具體比例主要依

違法行為之嚴重性確定，依歐盟 EDPB 指引，則允許考量違法行為人之規模，進一步調整罰鍰基本金額。新加坡係依違法行為嚴重性，由 PDPC 衡酌確定罰鍰基本金額，但未明定嚴重性與罰鍰基本金額間之定量關係。

與前述國家（地區）不同，我國公平交易法第 40 條之罰鍰計算方式中，罰鍰基本金額之計算與法定罰鍰上限（固定金額或銷售額之一定比例）無直接關聯，而是以違法行為於違法期間內「所獲銷售金額」的一定比例計算之。由南韓 2023 年修正案之文意觀察，似改採公平交易法之類似模式，以「相關銷售額」為罰鍰基本金額之計算基礎（第 64-2 條第 2 項），以「整體銷售額」之一定比例為法定上限（第 64-2 條第 3 項），然對於新法下罰鍰法定上限是否亦應以「相關銷售額」為計算基礎，實務從業者有不同解讀⁸⁴。南韓未來將如何執行新法規定，有待個資法施行令及計算基準之修正。

2. 法定罰鍰上限

浮動裁罰上限制度中，法定罰鍰金額上限須依行為人之具體情形個案計算。對此，南韓 2020 年 PIPA 第 39 條之 15 係以違法行為之「相關銷售額」為計算基礎。相較之下，歐盟、新加坡、南韓 2020 年 PIPA 第 28 條之 6 及 2023 年修正案，以及我國公平交易法第 40 條，

⁸⁴ Lee & Co., Second Major Amendment to the Personal Information Protection Act Passed by National Assembly (I), https://www.leeko.com/news/dpc/202302_e/dpc2302_e.pdf; Bae, Kim & Lee LLC, Korea passes extensive amendments to data privacy law, <https://www.lexology.com/library/detail.aspx?g=d253d033-68d0-4ba5-b1dd-c77dad6f35e5>.

皆以違法行為人之「年營業額（整體銷售額）」為計算基礎，但年營業額之具體計算方法不同。

年營業額之「主體範圍」方面，歐盟從經濟意義角度認定違法行為人，因此，對於集團公司而言，「年營業額」可將母公司與子公司之營業額合併計算。我國公平交易法第 40 條第 3 項授權訂定之罰鍰辦法則明確以法人地位認定違法行為人，故母公司與子公司之營業額不得合併計算。新加坡和南韓則未見此方面之具體討論。

年營業額之「地域範圍」方面，歐盟明文規定以「全球年營業額」為基礎，新加坡則明文以「境內年營業額」為計算基礎。我國公平交易法第 40 條及公平會罰鍰辦法雖對此無明文規定，然從實務案例觀察，於裁罰對象為外國公司時，得以該公司之境外營業額為計算基礎。南韓法中未見此方面之具體討論。

年營業額之「時間範圍」方面，歐盟、新加坡和我國公平交易法皆以「裁罰決定作出時」為時間基準，計算前一會計年度之營業額。南韓 2020 年 PIPA 第 28 條之 6 的整體銷售額，則是以前三年之平均銷售額計算，且從施行令第 29 條之 6 第 1 項觀察，其計算時點似以「違法行為時」為準。

（三）加重或減輕事由

本研究所涉之先進國家個資法之罰則規範，皆以法律形式明定主管機關裁處罰鍰時應考量之加重或減輕事由。其中，歐盟和新加坡皆採「例示+開放性事由」之模式，在列舉考量事由之同時，明文允許主管機關考量其他未列舉之事由。南韓 2020 年 PIPA 雖未規定其所列事由為例示性質，但施行令及主管機關之課賦基準皆包含法律未規

定之考量事由。南韓 2023 年修正案增列計算罰鍰金額之諸多事由，並明定主管機關依職權免處罰鍰之考量要素，但仍未規定開放性事由。未來南韓實務上是否將繼續以施行令、課賦基準等方式，納入其他考量事由，有待後續觀察。相較之下，我國公平交易法第 40 條並未列舉考量事由，而是授權主管機關訂定計算辦法。依公平會罰鍰辦法第 2 條及第 6 條，無論是「情節重大」之認定（確定個案中浮動上限適用與否），或罰鍰金額之調整（確定個案之罰鍰金額），似皆採完全列舉模式，而未保留主管機關依個案情形考量列舉範圍外其他事由之空間。

就加重或減輕事由之內容而言，歐盟、新加坡與南韓法律所列之事由有一定共通性。概言之，在計算罰鍰基本金額階段，通常綜合考量違法行為之性質、影響、持續期間、所涉個資類型、故意或過失程度等，判斷違法行為之嚴重性。在罰鍰金額之調整階段，則考慮行為人對主管機關之配合程度、對違法行為之補救措施、個資保護措施整體狀況、此前之違法情事等。在確定最終罰鍰金額階段，則考量當事人之資力、違法行為之社會經濟背景等，評估罰鍰金額之有效性、合比例性與嚇阻性。我國公平交易法下，公平會罰鍰辦法所列之事由雖係針對破壞競爭秩序行為所涉，但整體邏輯類似。

第三節 針對我國具體建議

（一）罰鍰制度之整體設計

1. 罰鍰之固定上限與下限

如前文所分析，本研究所涉之先進國家個資法，對違反個資保護規範行為之罰鍰固定上限，遠超我國現行個資法。就單純數值之比較，歐盟、新加坡及南韓對事業罰鍰之「最低」固定上限，為我國個資法「最高」罰鍰上限之幾十倍甚至數百倍。如以同類違法行為之罰鍰上限為視角，我國與先進國家之落差更為明顯，最高可相差千倍以上。

罰鍰上限之訂定，固屬一國立法政策之決定範圍，應由立法者依該國社會之價值追求、經濟發展水平等訂定，而不必然須與他國水準相符。然就我國近期社會現實觀察，與遵循個資法規範所需之成本、違反個資法行為所造成之直接及間接損害相比，個資法對違法行為之行政罰鍰上限顯然過輕⁸⁵，加之個資當事人對違反個資法行為之民事求償面臨難以證明損害或因果關係、訴訟程序漫長等缺陷⁸⁶，違反個資法難以產生有嚇阻性之後果，不僅不符社會期待，亦導致蒐集機關難有落實個資保護規範之誘因，主管機關缺乏有效執法之工具，從而損害民眾之個資保護權益。因此，我國似可考慮參考先進國家之個資法規範，適當提高罰鍰上限，賦予主管機關更有力之執法工具，以落實個資法之保護目的。提高後罰鍰上限之具體金額，應可參酌個資蒐集機關遵循個資法之成本、對罰鍰之承受能力、社會通念下違反個資法行為應受責難之程度、其他法規範規定之罰鍰水準等，綜合判斷決定。

⁸⁵ 洩個資僅罰 20 萬太輕 立委擬修法嚴懲：業者根本不痛不癢
(2023/02/13)，自由時報，

<https://news.ltn.com.tw/news/politics/breakingnews/4209374>.

⁸⁶ 例如，2017 年雄獅旅行社個資外洩相關訴訟中，消費者文教基金會（消基會）於 2018 年 3 月代表 25 名消費者提起團體訴訟，法院於 2019 年 11 月方作出消基會敗訴之判決，其理由之一為，消費者未證明其所受損害與雄獅旅行社個資外洩間有因果關係，臺灣士林地方法院 107 年度消字第 6 號民事判決參照。

另一方面，與我國不同，本研究所涉之先進國家個資法之行政罰鍰規範，皆未規定罰鍰金額下限，且在實務中，各國主管機關針對非營利組織、個人等之違法行為，不乏科處低於我國罰鍰下限之實例。考量我國現行法規範下，主管機關對於欠缺法律依據而蒐集、處理或（目的外）利用個資等行為，並無衡酌個案情形而不科處罰鍰之裁量權，如我國擬全面強化個資法之執法作業，似可考量放寬或移除罰鍰下限規範，或授權主管機關於個案中裁量減輕或免予處罰，以確保個案中罰鍰金額合乎比例。

2. 違法行為之分類

違法行為之分類方面，本研究所涉之先進國家個資法規範，可劃分為兩類。歐盟 GDPR 和南韓 2020 年 PIPA 在法律文本中，即針對違法行為之內容或違法行為人類別，分設不同之罰鍰額度。新加坡 PDPA 和南韓 2023 修正案則未設分類，各類違法行為皆適用同一罰鍰額度。

我國個資法第 47 條、第 48 條係採類似歐盟之模式，針對無法律依據蒐集、處理或（目的外）利用個人資料之行為，設定較高之罰鍰額度，而針對違反當事人權利行使或個資安全維護規範⁸⁷之行為，設定較低之罰鍰額度。

法律針對不同違法行為規定不同罰鍰額度，應與該違法行為背離法規範目的之嚴重程度相當。而違法行為對法規範目的之背離程度，

⁸⁷ 本研究係以 105 年施行之個資法為研析對象。本研究報告撰寫完成後，立法院於 112 年 5 月 16 日三讀通過個資法第 48 條修正案，經總統 112 年 5 月 31 日公布修正，自 112 年 6 月 2 日起生效，針對違反個資法第 27 條之行為，規定最高可處 1500 萬元之罰鍰，詳如前註 77 所示。

應考量特定法制環境與社會背景下對該行為之可非難程度。以歐盟 GDPR 之分類為例，個人資料受保護之權利（包括對個人資料之存取權與更正權，以及由獨立機關確保遵循）乃「歐聯基本權利憲章」所明定之基本權⁸⁸。或許是因為如此，GDPR 對於違反當事人權利行使規範之行為，規定較高之罰鍰金額上限，並將未能遵循主管機關糾正命令之行為，列為單獨之違法樣態，亦適用較高之罰鍰金額上限。我國似可依類似意旨，評估調整個資法第 47 條、第 48 條對違法行為之分類，或針對拒不遵守主管機關限期改正命令之行為，加重罰鍰金額。

3. 科處罰鍰之裁量權

如前文所述，本研究所涉之先進國家個資法之罰鍰規範，皆將行政罰鍰與命令糾正並列作為主管機關行政執法權力，允許主管機關裁量選擇是否單處或併處罰鍰或糾正措施，而未區別糾正措施與罰鍰之先備位適用順序，以使主管機關依個案情形，採取最有效、適當之執法措施。相較之下，我國個資法針對第 48 條所列之違法行為，則明定主管機關行政處罰權之裁量限制，要求主管機關須先命令限期改正，如違法行為人未遵守命令，方可科處罰鍰⁸⁹。

我國個資法之規範模式，恐難以實現對行為人之有效懲戒。例如，若行為人故意或重大過失未採取適當安全維護措施，致當事人個資遭外洩，主管機關依第 48 條規範，僅得命令改正，且只要行為人依命

⁸⁸ Charter of Fundamental Rights of the European Union, Article 8.

⁸⁹ 本研究係以 105 年施行之個資法為研析對象。本研究報告撰寫完成後，立法院於 112 年 5 月 16 日三讀通過個資法第 48 條修正案，經總統 112 年 5 月 31 日公布修正，自 112 年 6 月 2 日起生效，明定違反個資法第 27 條之行為，主管機關得逕處罰鍰，不以先行限期改正為必要，詳如前註 77 所示。

令改正完畢，主管機關即無權進一步科處罰鍰。然「命令改正」之本質，係要求行為人達成法令遵循，其作用僅在於回復遭破壞之法秩序，補救行為人違法行為所造成之後果，而對於較行為人已實施之違法行為，並無懲戒之效。縱主管機關於命令糾正時，一併依個資法第 25 條第 1 項第 4 款公布行為人違法情形、姓名或名稱、負責人等，亦僅屬名譽性處罰措施，懲戒效果有限，與行為人故意或重大過失實施違法行為之情節是否相當，容有疑問。執法措施懲戒性不足，將進一步影響行為人遵循第 48 條所列規範之積極性，不利於當事人相關權益（例如個資不被竊取、洩漏等）之保護，而有礙個資法立法目的之落實。

此外，我國個資法之規範模式，亦可能導致針對違法行為之執法措施不符社會期待，進而損及民眾對主管機關之信任。現行規範下，如發生重大個資侵害事件，無論個案中行為人之責任程度如何（例如故意或重大過失而未採取適當安全維護措施）、影響範圍如何（例如涉及巨量當事人之特種個資），主管機關囿於法律規範，仍無權直接科處罰鍰，僅能先命令糾正，至多同時公布違法情事⁹⁰。此將難免給民眾造成「輕放違法行為」之觀感，損害主管機關之公信力。

因此，為強化個資法執法措施之有效性，我國似可參酌先進國家規範，調整個資法第 48 條「先行命令改正」之要求，允許主管機關於個案中衡酌是否直接科處罰鍰。

⁹⁰ 同前註，本研究係以 105 年施行之個資法為研析對象。本研究報告撰寫完成後，立法院於 112 年 5 月 16 日三讀通過個資法第 48 條修正案，經總統 112 年 5 月 31 日公布修正，自 112 年 6 月 2 日起生效，明定違反個資法第 27 條之行為，主管機關得逕處罰鍰，不以先行限期改正為必要。

（二）浮動罰鍰上限之導入

如前文所分析，歐盟、新加坡、南韓等先進國家之個資法，皆採雙軌制罰鍰規範，在一定情形下適用浮動上限，以利實現個案中罰鍰措施之有效性、合比例性與嚇阻性。此外，我國法制中，亦已有採行雙軌制裁罰鍰規範之先例。在大型企業之個資侵害事故一再發生、大型企業採行安全維護措施之成本可能遠高於違法所受之罰鍰金額，民眾對個資法遵循需求更為迫切，然向大型企業求償之能力難度較高之背景下，我國個資法似可考量導入浮動罰鍰上限，使罰鍰金額與違法行為人之收益成正相關，強化罰鍰措施之嚇阻性，以收督促遵循之效。

1. 浮動上限之規範模式

本研究所涉之先進國家個資法雙軌制裁罰鍰規範，其浮動上限之規範模式，可大致分為兩類。歐盟、新加坡係以固定罰鍰金額上限為原則，於行為人之年營業額達較高水準時，以浮動上限為輔助；南韓則是以浮動上限為原則，於難以計算浮動上限時，例外適用固定上限。

如我國個資法擬導入雙軌制裁罰鍰設計，應以歐盟、新加坡模式較為可採。一方面，歐盟、新加坡浮動上限制度之目的，係在行為人之規模與承受能力較高時，確保罰鍰措施之有效性與嚇阻性，此與我國社會對個資法裁罰規範之需求相一致。另一方面，我國現行個資法第 47 條、第 48 條已設有固定罰鍰金額上限，公平交易法第 40 條亦是以浮動上限為輔助。固定上限為原則、浮動上限為例外之模式，較符合我國現行立法之習慣，利於提升人民對違法後果之預見性，且可減緩修法對產業與社會之衝擊。

如我國個資法擬參酌歐盟或新加坡模式，導入雙軌制裁罰設計，浮動上限之計算基礎，亦宜參照歐盟或新加坡模式，以違法行為人之年營業額為準，而無需區分相關銷售額或無關銷售額。原因在於，我國導入浮動上限之主要目的，係為了促使大型企業落實個資法遵循作為，以企業之年營業額計算浮動上限，罰鍰金額與企業規模直接相關，利於實現個案中罰鍰措施之有效性與嚇阻性。且同一企業遵循個資保護規範之能力，並不因該個資蒐集、處理或利用行為能否產生銷售收入而有差別，如將浮動上限之年營業額計算限於相關銷售額，可能造成企業不合理區別對待不同個資當事人之保護水準，而有違反平等原則之虞。此外，個資蒐集、處理或利用存在於企業營運之各個環節，個資法違法行為與企業銷售收入之關聯可能在事實面難以區分，以年營業額為浮動上限之計算基礎，亦可避免「相關銷售額」之範圍爭議。

在採年營業額為浮動上限計算基礎之前提下，年營業額之具體計算方式（例如時間基準、地域範圍、集團公司年營業額之計算方式等），可參酌公平交易法第 40 條第 3 項之立法模式，授權個資法解釋機關訂定。如個資法修正時，已依憲法法庭判決設立個資保護專責主管機關，則可授權該專責機關訂定。

2. 浮動上限之適用範圍

本研究所涉之先進國家個資法雙軌制裁罰規範，除南韓 2020 年 PIPA 係局部採用雙軌裁罰制度外，歐盟、新加坡以及南韓 2023 年修正案係全面採用雙軌裁罰制度，各類行為人之各類違法行為，皆有浮動上限之適用。且新加坡、南韓皆係透過近年之修法，導入全面性浮動上限，全面性雙軌裁罰制度似可認為已成國際趨勢。

相較之下，我國公平交易法則是採用雙軌裁罰制度，僅針對性質最為嚴重之特定違法行為（違反第 9 條和第 15 條），規定罰鍰之浮動上限。

如我國個資法擬參酌歐盟或新加坡模式，導入雙軌制裁罰設計，對一定規模以上之違法行為人提高罰鍰法定上限，應以全面性浮動上限較為可採。主要原因在於，我國社會對於個資法裁罰規範最迫切之修法需求，乃上修違反個資安全維護規範之罰鍰額度⁹¹，促使業者採取適足安全維護措施，遏制個資外洩事件。因此，如參酌歐盟或新加坡模式導入浮動上限，其適用範圍應包含違反個資安全維護規範之行為。然而，我國現行個資法第 47 條及第 48 條針對不同違法行為，區分不同裁罰上限。違反個資安全維護規範及當事人權利行使規範之裁罰上限較低（第 48 條），違反個資蒐集處理利用適法性規範之裁罰上限則較高（第 47 條）。因此，在保持個資法裁罰規範現行結構之前提下，如於第 48 條導入浮動上限制度，則第 47 條亦應同步導入，以維護規範體系之一致性。

更進一步而言，如調整個資法對違法行為之分類，亦不宜僅就個資安全維護規範導入浮動上限。蓋從違法行為的對基本權的侵害觀之，違反個資蒐集處理利用適法性或當事人權利行使規範，將直接限制乃至剝奪個資當事人對其個資揭露與使用之知悉權，以及事前、事中與事後之控制權⁹²，應屬對個人資料自主權之直接侵害；相較之下，違

⁹¹ 本研究係以 105 年施行之個資法為研析對象。本研究報告撰寫完成後，立法院於 112 年 5 月 16 日三讀通過個資法第 48 條修正案，經總統 112 年 5 月 31 日公布修正，自 112 年 6 月 2 日起生效，針對「違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法」之行為，將罰鍰上限提升至最高 1500 萬元，詳如前註 77 所示。

⁹² 司法院釋字第 603 號解釋、憲法法庭 111 年憲判字第 13 號判決參照。

反個資安全維護規範之行為，自身通常不致影響個資當事人對其個資利用狀況之知悉與控制，而是升高個資遭非法蒐集、處理或利用之風險，可謂間接侵害個資當事人之個人資料自主權。因此，如僅針對個資安全維護規範導入浮動上限，恐有輕重失衡之虞。

3. 浮動上限之適用前提

對於適用浮動上限之違法行為，歐盟、新加坡及南韓未在法律層面對浮動上限之適用另設限制條件。相較之下，我國公平交易法第 40 條第 2 項則明文要求浮動上限之適用，以違法行為「情節重大」者為限。

關於是否需參考公平交易法第 40 條第 2 項，以法律明定浮動上限之適用以「情節重大」為限，立法者似可衡酌我國社會之個資保護需求及業者之承受能力等因素，綜合判斷之。詳言之，如明定以「情節重大」為限，可將大型業者未達重大程度之違法行為，直接排除於浮動上限適用範圍外，較能降低對產業之衝擊。然此種方式下，大型業者之違法行為如未達重大程度，仍適用固定上限，個案中罰鍰之有效性及嚇阻性可能不足，從而不利於個資保護規範之落實。相較之下，如未明定以「情節重大」為限，而是委諸主管機關之個案裁量，可提供主管機關採行執法措施時較高之靈活性，而利於規範保護目的之有效實現。然此種方式對產業衝擊較大，修法過程可能面臨較高阻力。

值得注意的是，歐盟、新加坡與南韓雖未於法律層面明定浮動上限之適用以「情節重大」者為限，然其主管機關仍於實務操作指引中，將違法行為之情節作為個案罰鍰金額之重要考量。如我國立法者經衡量判斷後，未於個資法中明定浮動上限之適用以「情節重大」為限，

亦可授權主管機關訂定公平會罰鍰辦法或裁量基準等，明確科處罰鍰過程中不同違法情節之影響，提升對行為人之可預見性。

（三）配套措施

1. 罰鍰金額之計算方式

本研究所涉之先進國家，皆就罰鍰措施訂定個資法之子法規，或由主管機關訂定相關指引，以提升民眾對罰鍰措施之可預見性，並促進不同案件（不同會員國主管機關）裁量基準之統一。

我國現行個資法雖授權訂定施行細則，然並未就行政罰鍰相關規定作補充規範。而從我國通常立法習慣觀察，法律明確授權訂定罰鍰相關之法規命令，除罰鍰計算方法較複雜之情形外（例如公平交易法第 40 條），多見於違法樣態較為複雜、情節及嚴重性落差較大之食品安全、環境污染等領域⁹³。考量違反個資法行為之樣態相對單純，如我國個資法僅修法調整固定罰鍰之上限或下限，似無須特別授權訂定公平會罰鍰辦法。然如導入雙軌制裁罰規範，則宜參酌公平交易法第 40 條，授權訂定配套子法規，明確罰鍰金額之計算步驟、浮動上限之計算方式等，以利提升新型裁罰規範之明確性。

2. 加重減輕事由

本研究所涉之先進國家個資法規範，皆以法律形式明定主管機關裁處罰鍰時應考量之加重或減輕事由。相較之下，依我國立法習慣，

⁹³ 例如，食品安全衛生管理法第四十四條第一項罰鍰裁罰標準（食品安全衛生管理法第四十四條第二項授權訂定）、違反廢棄物清理法罰鍰額度裁罰準則（廢棄物清理法第六十三條之一第一項授權訂定）、違反水污染防治法罰鍰額度裁罰準則（水污染防治法第六十六條之一第二項授權訂定）等。

除行政罰法第 18 條第 1 項及第 2 項之規範外，較少直接於法律中規定科處罰鍰之審酌事項或加重減輕事由⁹⁴，而多以授權訂定之子法規加以規範⁹⁵。因此，如我國個資法未來導入雙軌制裁罰規範，宜參酌公平交易法第 40 條第 3 項規定，授權訂定配套子法規，並由主管機關於子法規中列舉計算罰鍰金額之審酌事由。如擬全面性進一步明確科處罰鍰時之加重或減輕事由，則宜參酌公平交易法施行細則第 36 條之模式，以修正個資法施行細則方式為之。

3. 修正條文之施行安排

如前文所述，新加坡為減緩修法條文對社會及產業之衝擊，對 PDPA 之修法歷程採分階段進行模式，以第一階段細化行政罰鍰之科處程序及審酌事由規定；第二階段則完整落實修法目的，導入雙軌制罰鍰規範，針對大型業者實質提高罰鍰上限。行政裁罰相關之修法條文正式通過至完整施行，歷時將近 2 年。歐盟 GDPR 雖未採分階段施行之模式，然就其全部規範訂有施行過渡期，從訂定到正式施行，歷時超過 2 年。

如我國個資法擬同時提升罰鍰金額固定上限，並針對一定規模以上之業者導入浮動上限制度，則宜參酌新加坡修法歷程中的分階段施行方式，首先施行固定上限之修正條文，於經歷一定過渡期後，再施行浮動上限之修正條文，並由主管機關提前擬定配套子法規或指引，

⁹⁴ 少數法規例如，勞動基準法第 80-1 條第 2 項、勞工職業災害保險及保護法第 100 條第 2 項。

⁹⁵ 除前文已列舉之公平會罰鍰辦法，以及食品安全、環境保護領域之罰鍰計算基準外，亦包括：公平交易法施行細則第 36 條、多層次傳銷管理法施行細則第 19 條、教保相關人員違法事件調查處理辦法第 29 條等。

與相應修正條文一併施行，以利提供業者調適之適當期間，並提升新修條文執行措施之可預見性。

（四）修法條文草案

本研究基於前述比較研究與分析，提供個資法行政罰鍰相關規範修正條文草案建議如下。

表 1 行政罰鍰相關修正條文草案對照表

修正條文	現行條文 ⁹⁶	說明
第四十七條 I. 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣<u>五百萬元</u>以下罰鍰，並令限期改正，屆期未改正者，<u>繼續限期令改正，並按次處新臺幣十萬元以上二千萬元以下罰鍰</u>： 一、違反第六條第一項規定。 二、違反第十九條規定。 三、違反第二十條第一項規定。 四、違反中央目的事業主管機關依第二十	第四十七條 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣<u>五萬元以上五十萬元</u>以下罰鍰，並令限期改正，屆期未改正者，<u>按次處罰之</u>： 一、違反第六條第一項規定。 二、違反第十九條規定。 三、違反第二十條第一項規定。 四、違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或處分。	一、對於違反本法蒐集、處理、利用或國際傳輸特種或一般個資之行為，現行最高僅可處以新臺幣五十萬元罰鍰，與遵守本法規範之成本或違法行為可獲得之利益顯不相當，而難收督促遵循之效，爰修正第一項，提升罰鍰金額上限，並就屆期未改正者，加重處罰額度。又考量個案中違法行為情節、所應受責難程度及行為人資力可能差異甚大，故刪除罰鍰金額下限規定，以利裁罰處分與其行為之情

⁹⁶ 本研究係以 105 年施行之個資法為研析對象。本研究報告撰寫完成後，立法院於 112 年 5 月 16 日三讀通過個資法第 48 條修正案，經總統 112 年 5 月 31 日公布修正，自 112 年 6 月 2 日起生效，針對「違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法」之罰則，刪除原個資法第 48 條第 4 款，並增訂第 48 條第 2 項、第 3 項，詳如前註 77 所示。

修正條文	現行條文 ⁹⁶	說明
一條規定限制國際傳輸之命令或處分。 II. <u>前項之非公務機關為事業者，得處該事業上一會計年度收入總額百分之二以下罰鍰，不受前項罰鍰金額限制。</u> <u>本條及第四十八條第二項之事業，係指：</u> 一、<u>公司。</u> 二、<u>獨資或合夥之工商行號。</u> 三、<u>執行業務者。</u> 四、<u>其他提供商品或服務從事交易之人或團體。</u> III. <u>本條至第五十條罰鍰計算之辦法，由行政院指定機關定之。</u>		節輕重相當。 二、數位經濟時代，非公務機關規模大小與對資料之蒐集處理利用數量、落實遵循之能力、違法行為造成之當事人權益侵害成正相關，故參酌歐盟GDPR、新加坡《個人資料保護法》(PDPA)等關於行政罰鍰之規範，增訂第二項，規定事業年收入總額之百分之二超過前項罰鍰金額上限者，不受前項罰鍰金額限制，並增訂事業之範圍。 三、增訂第三項，授權行政院指定機關訂定本法罰鍰之計算辦法，以利提升罰鍰措施計算方法之明確性。
第四十八條	第四十八條	一、修正第一項，提升罰

修正條文	現行條文 ⁹⁶	說明
I. 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處<u>新臺幣二百萬元以下罰鍰</u>，並令限期改正，屆期未改正者，<u>繼續限期令改正</u>，並按次處新臺幣<u>十萬元以上一千萬元以下罰鍰</u>： 一、違反第八條或第九條規定。 二、違反第十條、第十一條、第十二條或第十三條規定。 三、違反第二十條第二項或第三項規定。 四、違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。	非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣<u>二萬元以上二十萬元以下罰鍰</u>： 一、違反第八條或第九條規定。 二、違反第十條、第十一條、第十二條或第十三條規定。 三、違反第二十條第二項或第三項規定。 四、違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。	鍰金額上限，就屆期未改正者，加重處罰額度，以利促進遵循。刪除罰鍰金額下限規定，以利裁罰與違法情節相當。 二、增訂第二項，規定事業年收入總額之百分之一超過前項罰鍰金額上限者，不受前項罰鍰金額限制，以提升裁罰處分之嚇阻性。

修正條文	現行條文 ⁹⁶	說明
II. <u>前項之非公務機關為 事業，得處該事業上 一會計年度收入總額 百分之一以下罰鍰，不 受前項罰鍰金額限制。</u>		

第五章 結論

綜合前文之比較分析，本研究參酌歐盟、新加坡、南韓等先進國家個資法之雙軌制行政罰鍰規範，以及我國法制中既有之雙軌制罰鍰制度，建議我國可考量從下列方面修正個資法行政罰鍰條文，以利合理強化業者個資保護責任，回應社會期待並促進法規遵循：

1. 我國個資法區分不同違法行為內容，分別規定 50 萬元及 20 萬元之固定罰鍰上限，與遵循個資法規範所需之成本、違反個資法行為所造成之直接及間接損害相比，現行罰鍰上限過低，難以對違法行為產生有嚇阻性之後果，不僅不符社會期待，亦導致蒐集機關難有落實個資保護規範之誘因。因此，我國似可綜合評估遵循個資法之成本、對罰鍰之承受能力、社會通念下違反個資法行為應受責難之程度、其他法規範規定之罰鍰水準等因素，並參考先進國家之個資法規範，適當提高罰鍰上限，賦予主管機關更有力之執法工具，以落實個資法之保護目的。
2. 我國個資法第 47 條針對欠缺法律依據而蒐集、處理或（目的外）利用個資等行為，訂有 5 萬元罰鍰金額下限，且主管機關並無衡酌個案情形而不科處罰鍰之裁量權。如我國擬全面強化個資法之執法作業，似可考量放寬或移除罰鍰下限規範，或授權主管機關於個案中裁量減輕或免予處罰，以確保個案中罰鍰金額合乎比例。

3. 我國個資法第 48 條針對個資安全維護措施不足⁹⁷、未將個資侵害事故通知個資當事人、未盡告知義務、未遵循當事人權利行使請求等違法行為，要求主管機關須先命令限期改正，如違法行為人未遵守命令，方可科處罰鍰。此種規範模式可能損害執法措施之有效性，且可能因執法措施不符社會期待而損及主管機關之公信力。因此，我國似可參酌先進國家規範，調整個資法第 48 條「先行命令改正」之要求，允許主管機關於個案中衡酌是否直接科處罰鍰。
4. 針對大型企業採行安全維護措施之成本可能遠高於違法所受之罰鍰金額之情形⁹⁸，我國個資法似可考量導入浮動罰鍰上限，使罰鍰金額與違法行為人之收益成正相關，強化罰鍰措施之嚇阻性，以收督促遵循之效。在制度設計中，宜以固定罰鍰金額上限為原則，於行為人之年營業額達較高水準時，以浮動上限為輔助，且浮動上限之計算，宜以整體營業額為依據，以避免計算基礎之爭議。

⁹⁷ 本研究係以 105 年施行之個資法為研析對象。本研究報告撰寫完成後，立法院於 112 年 5 月 16 日三讀通過個資法第 48 條修正案，經總統 112 年 5 月 31 日公布修正，自 112 年 6 月 2 日起生效，針對「違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法」之行為，已不再要求主管機關先命令改正，詳如前註 77 所示。

⁹⁸ 本研究係以 105 年施行之個資法為研析對象。本研究報告撰寫完成後，立法院於 112 年 5 月 16 日三讀通過個資法第 48 條修正案，經總統 112 年 5 月 31 日公布修正，自 112 年 6 月 2 日起生效，針對「違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法」之行為，將罰鍰上限提升至最高 1500 萬元，詳如前註 77 所示。

5. 作為行政罰鍰規範修正之配套措施，我國個資法可考量授權訂定配套子法規，明確罰鍰金額之計算步驟、浮動上限之計算方式、加重減輕事由等，以利提升新修裁罰規範之明確性。
6. 為減緩修法措施對產業之衝擊，我國可考量分階段實施新法。例如，若同時提升罰鍰金額固定上限，並針對一定規模以上之業者導入浮動上限制度，可首先施行固定上限之修正條文，於經歷一定過渡期後，再施行浮動上限之修正條文，並由主管機關提前擬定配套子法規或指引，與相應修正條文一併施行，以利提供業者調適之適當期間，並提升新修條文執行措施之可預見性。

參考文獻

法律和立法草案

1. 中華民國，公平交易法。
2. 中華民國，公平交易法施行細則。
3. 中華民國，司法院釋字第 603 號解釋。
4. 中華民國，多層次傳銷管理法施行細則。
5. 中華民國，行政罰法。
6. 中華民國，食品安全衛生管理法。
7. 中華民國，個人資料保護法。
8. 中華民國，海關緝私條例。
9. 中華民國，教保相關人員違法事件調查處理辦法。
10. 中華民國，勞工職業災害保險及保護法。
11. 中華民國，勞動基準法。
12. 中華民國，違反公平交易法第十條及第十四條情節重大案件之裁處罰鍰計算辦法。
13. 中華民國，違反水污染防治法罰鍰額度裁罰準則。
14. 中華民國，違反廢棄物清理法罰鍰額度裁罰準則。
15. 南韓，個人情報保護委員會，「조문별
제개정이유서(개인정보보호법 일부개정법률안)(최종)」，
<https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS061&mCode=C010010000&nttId=7059#LINK>.

16. 南韓，個人情報保護委員會，違反個人情報保護相關法規之課徵金課賦基準。
17. 南韓，情報通信網法（2008 年 6 月 13 日法律第 9119 號）。
18. 南韓，情報通信網法（2014 年 5 月 28 日法律第 12681 號）。
19. Australian Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022.
20. European Union, Charter of Fundamental Rights of the European Union.
21. European Union, 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.
22. European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
23. MCI of Singapore, Closing Note to the Public Consultation on draft Personal Data Protection (Amendment) Bill including related amendments to the Spam Control Act (05 Oct 2020), [https://www.mci.gov.sg/public-consultations/public-consultation-items/closing-note-to-pc-on-draft-pdp-\(amendment\)-bill-including-related-amendments-to-spam-control-act](https://www.mci.gov.sg/public-consultations/public-consultation-items/closing-note-to-pc-on-draft-pdp-(amendment)-bill-including-related-amendments-to-spam-control-act).

24. MCI of Singapore, Personal Data Protection (Amendment) Act 2020 (Commencement) Notification 2021 (27 January 2021), <https://sso.agc.gov.sg//SL/S60-2021?DocDate=20210129>.
25. MCI of Singapore, Public Consultation on the Draft Personal Data Protection (Amendment) Bill, Personal Data Protection (Amendment) Bill 2020, <https://www.mci.gov.sg/public-consultations/public-consultation-items/public-consultation-on-the-draft-personal-data-protection-amendment-bill>.
26. Singapore, Personal Data Protection (Amendment) Act 2020.
27. Singapore, Personal Data Protection (Enforcement) Regulations 2021.
28. Singapore, Personal Data Protection Act 2012.
29. 개인정보 보호법 전면개정, 데이터 신경제 시대 열린다, <https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=8674>.
30. 「개인정보 보호법」 일부개정법률(안) 입법예고, <https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS061&mCode=C010010000&nttId=7059#LINK>.

實務案例及判決

31. 中華民國，公平交易委員會公處字第 104139 號處分書。
32. 中華民國，公平交易委員會公處字第 104140 號處分書。
33. 中華民國，最高行政法院 108 年度判字第 597 號判決。
34. 中華民國，臺北高等行政法院 105 年度訴字第 250 號判決

35. 中華民國，臺北高等行政法院 105 年度訴字第 284 號判決。
36. 中華民國，臺灣士林地方法院 107 年度消字第 6 號民事判決。
37. 中華民國，憲法法庭 111 年憲判字第 13 號判決。
38. 南韓，憲法裁判所 2020 헌마 259 判決。
39. Belgian Gegevensbeschermingsautoriteit, DOS-2019-04191 (mei 2020),
<https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-28-2020.pdf>.
40. CJEU, Case C-300/21 - Österreichische Post (Préjudice moral lié au traitement de données personnelles), Opinion Of Advocate General (6 October 2022),
<https://curia.europa.eu/juris/document/document.jsf?text=&docid=266842&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3719836>.
41. CJEU, Case C-97/08 P, Akzo Nobel NV and Others v Commission of the European Communities, Judgment (10 September 2009),
<https://curia.europa.eu/juris/document/document.jsf?text=&docid=72629&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2232090>.
42. CJEU, Case T-709/21, WhatsApp Ireland v EDPB, Action brought on 1 November 2021,
<https://curia.europa.eu/juris/document/document.jsf?text=&docid=251>

[744&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1
&cid=2953747](https://curia.europa.eu/juris/document/document.jsf?text=&docid=268419&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=2953747).

43. CJEU, Case T-709/21, WhatsApp Ireland v EDPB, Order of The General Court, 7 December 2022, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=268419&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2953747>.
44. EDPB, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR (28 July 2021) .
45. Irish DPC, Decision in the matter of MOVE Ireland, DPC Case Reference: IN-20-7-1 (20 August 2021), <https://www.dataprotection.ie/sites/default/files/uploads/2021-11/IN-20-7-1%20Move%20Irl%20Final%20Decision.pdf>.
46. Irish DPC, Decision in the matter of WhatsApp Ireland Limited made pursuant to Section 111 of the Data Protection Act 2018, https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf.
47. Singapore PDPC, Advance Home Tutors [2019] SGPDPC 35, Decision.
48. Singapore PDPC, Amicus Solutions Pte. Ltd. and Ivan Chua Lye Kiat [2019] SGPDPC 33, Decision.
49. Singapore PDPC, Aviva Ltd [2018] SGPDPC 4, Decision.

50. Singapore PDPC, Aviva Ltd and Toh-Shi Printing Singapore Pte Ltd [2016] SGPDPC 15, Decision.
51. Singapore PDPC, ComGateway (S) Pte. Ltd. [2017] SGPDPC 19, Decision.
52. Singapore PDPC, Creative Technology Ltd [2020] SGPDPC 1, Decision.
53. Singapore PDPC, DS Human Resource Pte. Ltd. [2019] SGPDPC 16, Decision.
54. Singapore PDPC, Institute of Singapore Chartered Accountants [2018] SGPDPC 28, Decision.
55. Singapore PDPC, Ninja Logistics Pte Ltd [2019] SGPDPC 39, Decision.
56. Singapore PDPC, O2 Advertising Pte. Ltd. [2019] SGPDPC 32, Decision.
57. Singapore PDPC, Option Gift Pte Ltd [2019] SGPDPC 10, Decision.
58. Singapore PDPC, Propnex Realty Pte Ltd [2017] SGPDPC 1, Decision.
59. Singapore PDPC, Sharon Assya Qadriyah Tang [2018] SGPDPC 1, Decision
60. Singapore PDPC, Singapore Health Services Pte. Ltd. and Integrated Health Information Systems Pte. Ltd. [2019] SGPDPC 3, Decision.
61. Singapore PDPC, Singapore Telecommunications Limited [2019] SGPDPC 49, Decision.

62. Singapore PDPC, SPH Magazines Pte Ltd [2020] SGPDPC 3, Decision.

63. Singapore PDPC, Zero1 Pte. Ltd. and XDEL Singapore Pte. Ltd. [2019] SGPDPC 37, Decision.

實務指引與工作文件

64. 南韓，個人情報保護委員會，「違反假名情報處理之課徵金基準制定案行政預告」公告，（2021 年 4 月 1 日），

<https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS061&mCode=C010010000&nttId=7242>.

65. EDPB, Guidelines 04/2022 on the calculation of administrative fines under the GDPR (12 May 2022),

https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf.

66. EU Commission, Commission Guidelines on the method of setting fines imposed pursuant to Article 23(2)(a) of Regulation No 1/2003 (2006/C 210/02),

<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52006XC0901%2801%29>.

67. PDPC, Guide on Active Enforcement (1 October 2022).

68. Singapore PDPC, Advisory Guidelines on Enforcement of Data Protection Provisions (October 2022),

<https://www.pdpc.gov.sg/guidelines-and-consultation/2020/02/advisory-guidelines-on-enforcement-of-data-protection-provisions>.

69. Singapore PDPC, Advisory Guidelines on the Do Not Call Provisions (1 February 2021), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-on-the-DNC-Provisions-1-Feb-2021.pdf>.

70. Singapore PDPC, Guide on Active Enforcement (October 2022), <https://www.pdpc.gov.sg/help-and-resources/2019/05/guide-on-active-enforcement>.

71. WP29, Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679 (WP 253) (3 October 2017).

其他參考資源

72. 中華民國，自由時報，「洩個資僅罰 20 萬太輕 立委擬修法嚴懲：業者根本不痛不癢」，（2023 年 2 月 13 日），
<https://news.ltn.com.tw/news/politics/breakingnews/4209374>.

73. 南韓，個人情報保護委員會，第 20 次全體會議，裁罰實務新聞稿，（2022 年 12 月 14 日），
<https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020000000&nttId=8357#LINK>.

74. 南韓，個人情報保護委員會，第 4 次全體會議，裁罰實務新聞稿，（2023 年 3 月 8 日），
<https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020000000&nttId=8680>.

75. Bae, Kim & Lee LLC, Korea passes extensive amendments to data privacy law,

<https://www.lexology.com/library/detail.aspx?g=d253d033-68d0-4ba5-b1dd-c77dad6f35e5>.

76. Irish DPC, Data Protection Commission announces decision in WhatsApp inquiry (02 September 2021),

<https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry>;

77. Lee & Co., Second Major Amendment to the Personal Information Protection Act Passed by National Assembly (I),

https://www.leeko.com/news/dpc/202302_e/dpc2302_e.pdf.

78. 「개인정보 보호·활용 포지티브섬 게임

왜야」 <https://shindonga.donga.com/3/all/13/4047763/1>.

79. 「주민등록번호 유출 등에 대한 과징금

부과기준」, <https://www.law.go.kr/LSW/admRulLsInfoP.do?admRulSeq=2100000215231>.

80. 개정 개인정보법 과징금 ‘조삼모사’ 논란에... 담당부처

답변은? <https://www.hani.co.kr/arti/economy/it/1082532.html>.

歐盟、南韓、新加坡個人資料保護法對於違反安全維護義務之行政處罰規定/葉奇鑫計畫主持 -- 初版. -- 臺北市：國發會，民 112.06

面：表，公分

編號：(112)005.0901

委託單位：國家發展委員會

受託單位：達文西個資暨高科技法律事務所

個人資料保護法

584.111

題名：歐盟、南韓、新加坡個人資料保護法對於違反安全維護義務之行政處罰規定

委託單位：國家發展委員會

受託單位：達文西個資暨高科技法律事務所

計畫主持人：葉奇鑫

出版機關：國家發展委員會

電話：02-23165300

地址：臺北市寶慶路 3 號

網址：<http://www.ndc.gov.tw/>

出版年月：中華民國 112 年 6 月

版次：初版

刷次：第 1 刷

編號：(112) 005.0901 (平裝)