國立臺灣大學進修推廣學院事業經營法務碩士在職學位學程

碩士論文

Professional Master's Program of Law in Business Administration

School of Professional Education and Continuing Studies

National Taiwan University

Master's Thesis

# 論電商平臺業者個資外洩之民事損害賠償責任

# On the Civil Liability for Damages Due to Data Breaches by E-commerce Platform Operators

葉長青

Chang-Ching Yeh

指導教授：吳從周 博士

Advisor: Chung-Jau Wu, Dr iur.

中華民國 114 年 6 月

June, 2025

doi:10.6342/NTU202501770

# 國立臺灣大學碩士學位論文
# 口試委員會審定書
## MASTER'S THESIS ACCEPTANCE CERTIFICATE
## NATIONAL TAIWAN UNIVERSITY

論電商平臺業者個資外洩之民事損害賠償責任

On the Civil Liability for Damages Due to Data Breaches by

E-commerce Platform Operators

本論文係葉長青（P12E42017）在國立臺灣大學事業經營法務碩士在職學位學程完成之碩士學位論文，於民國 114 年 6 月 17 日承下列考試委員審查通過及口試及格，特此證明。

The undersigned, appointed by the Professional Master's Program of Law in Business Administration on 17 June 2025, have examined a Master's Thesis entitled above presented by Chang-Ching Yeh （P12E42017） candidate and hereby certify that it is worthy of acceptance.

口試委員 Oral examination committee:

王化明　邱琦　周明恩

（指導教授 Advisor）

系（所、學位學程）主管 Director: 謝志煜



doi:10.6342/NTU202501770

# 誌謝

在本論文寫作完成之際，謹向在這段漫長歷程中給予我支持與鼓勵的親人、師長與夥伴們，致上最誠摯的感謝。

首先，我要感謝我最親愛的媽媽與姊姊，感謝你們始終如一的全力支持與理解。在我低潮沮喪時，總是你們給予我無條件的愛與陪伴，是你們讓我得以無後顧之憂地專注於學術研究，這份溫柔與堅定，是我能走到今天最重要的力量來源。

我也衷心感謝指導教授吳從周教授的悉心指導與啟發。教授嚴謹而深刻的學術態度、對法律問題精準的剖析視角，以及在我研究方向上提供的諸多指引，讓我得以在有限的篇幅中，試圖釐清複雜的法律爭點。每次討論中教授提出的提問與挑戰，都是促使我持續思辨、深化論述的動力來源。

同時，我要由衷感謝在共同研究與討論中攜手前行的神隊友—蘊涵、鼎超。你們不僅是學術上的最佳夥伴，也是在這段學習歷程中始終投入、可靠且專業的合作夥伴。無論是在討論中的觀點交流，或是在時程壓力下的相互協助，都讓我深感團隊合作的可貴與踏實。

亦感謝 PM「美味吃透透」的成員丞修、婉如、佳宏、易汝、昱彣、梓銜、陳芃，在壓力之餘能與你們共度美食時光、交換資料心得，甚至偶爾相約小旅行，這些看似日常的陪伴，卻成為我在論文路上最療癒與堅定的支撐。謝謝你們，讓我在追求學術的同時，也未曾遺落生活的豐富與溫度。

我也要感謝在 PM 學程中認識的寶藏同學千惠。溫柔、耐心的妳總是在我迷惘或焦慮時給予心靈上的支持與真誠的建議。我們徹夜長談、分享彼此的人生經歷與想法，在工作與學業壓力下，妳的陪伴讓我感受到溫暖與踏實。謝謝妳一路相伴，讓這段求學歲月變得更加有光。

特別感謝應璉，您在財務管理與策略管理領域展現出令人敬佩的深厚實力，不僅提供我許多精闢的見解與思維方向，更讓我在互動中學習良多、進步甚多。您的專業態度與清晰邏輯，是我努力追趕與效法的對象，衷心感謝這段期間的交流與啟發。



doi:10.6342/NTU202501770

謝謝你們，讓這段過程不再孤單，也賦予本論文成果更深層的意義。未來我將以此為起點，持續深化專業素養與思辨能力，期許自己在實務與學術領域中，成為值得信賴、持續成長的法律人。



doi:10.6342/NTU202501770

# 中文摘要

隨著數位經濟與電商產業蓬勃發展，企業大量蒐集與運用個人資料，帶來營運效率提升的同時，也加劇個資外洩風險，嚴重威脅消費者隱私與財產安全。近年來臺灣屢見重大個資外洩事件，引發社會高度關注，亦突顯現行法律在責任認定、損害救濟與制度設計上的不足與挑戰。

本研究旨在探討電商平台業者於個人資料外洩事件中所涉及的民事損害賠償責任，透過三重路徑展開：其一，分析歐盟 GDPR 第 82 條損害賠償制度之理論架構與法院判決發展，檢視控制者過失推定、非財產損害可賠性與損害賠償計算原則；其二，系統整理十二件臺灣法院個資外洩判決，分析法院對於過失責任、相當因果關係、舉證責任分配及損害範圍的認定標準與歧異見解；其三，檢視臺灣個人資料保護法第 27 條「適當安全維護措施」規範與施行細則內容，探討業者實務遵循困境及法律規範之模糊性。

研究結果指出，臺灣實務採行「過失推定」模式，惟各級法院在因果關係判斷與損害範圍認定上歧見甚大，致使企業法律風險難以預測。相較之下，歐盟 GDPR 強調法律義務明確化、精神損害補償與預防性制度設計，具有可供我國借鏡之價值。本文據此提出制度建議，包括：明確化安全維護標準、引進資料保護長與 DPIA 機制、強化事故通報義務、補強損害賠償體系，並健全獨立監理機構，以建立具前瞻性與可預期性的個資保護制度。

本研究期盼能為電商平台建立風險應對機制提供參考，並為臺灣未來個資法制改革方向提出具體建議，實現消費者權益保障與數位產業發展之雙重目標。

關鍵詞：電商平台、個人資料外洩、民事責任、GDPR、損害賠償



doi:10.6342/NTU202501770

# ABSTRACT

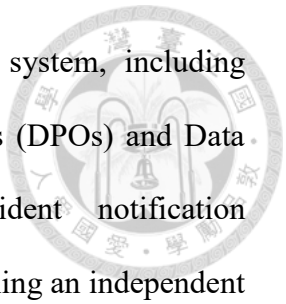
With the rapid development of the digital economy and e-commerce industry, businesses are collecting and utilizing vast amounts of personal data. While this practice enhances operational efficiency, it simultaneously increases the risk of data breaches, posing significant threats to consumer privacy and financial security. In recent years, Taiwan has witnessed a surge in high-profile personal data leak incidents, revealing critical deficiencies in the current legal framework regarding liability attribution, damage recovery, and institutional design.

This study explores the civil liability of e-commerce platform operators in the context of personal data breaches through a three-pronged approach. First, it examines the structure and judicial interpretation of Article 82 of the EU General Data Protection Regulation (GDPR), focusing on the presumption of fault, compensability of non-material damage, and principles for calculating damages. Second, it systematically analyzes twelve Taiwanese court decisions involving data breach cases, highlighting divergent judicial approaches to negligence, causation, burden of proof, and scope of compensable damages. Third, it evaluates the regulatory requirements under Article 27 of Taiwan's Personal Data Protection Act and its implementing rules, discussing the ambiguity and compliance challenges faced by businesses in practice.

The research finds that while Taiwanese courts generally adopt a presumption of negligence, they show substantial inconsistency in assessing causation and damages, resulting in significant legal uncertainty for businesses. In contrast, the GDPR provides a clearer and more stringent liability framework, emphasizing legal certainty, compensation for emotional distress, and preventive governance. Drawing from this comparative



doi:10.6342/NTU202501770



analysis, the study proposes several reforms for Taiwan's legal system, including clarifying security obligations, introducing Data Protection Officers (DPOs) and Data Protection Impact Assessments (DPIAs), strengthening incident notification requirements, enhancing the civil compensation regime, and establishing an independent regulatory authority.

This research aims to offer practical guidance for e-commerce platforms in managing data breach risks and to contribute concrete recommendations for future reforms of Taiwan's personal data protection regime, striving to balance consumer rights protection and digital industry development.

**Keywords:** E-commerce platforms, personal data breach, civil liability, GDPR Article 82, damage compensation



**doi:10.6342/NTU202501770**

# 簡目

**第一章　緒論 ..... 1**

第一節　研究背景與動機 ..... 1

第二節　研究目的 ..... 4

第三節　研究方法 ..... 5

第四節　研究架構 ..... 5

**第二章　歐盟一般資料保護規範（GDPR）下企業個資洩漏之責任 ..... 8**

第一節　GDPR 規定概述 ..... 8

第二節　GDPR 核心原則與個人權利保障 ..... 13

第三節　GDPR 下損害賠償責任的認定與實務發展 ..... 17

**第三章　我國個資法規定與電商平台業者之個資管理義務 ..... 35**

第一節　個資法之立法背景與沿革 ..... 35

第二節　個資法規範電商業者之個資管理義務 ..... 38

第三節　企業如何符合個資法第 27 條適當安全維護措施之標準 ..... 41

**第四章　我國個人資料外洩民事損害賠償責任之實務判決分析 ..... 47**

第一節　我國法院實務判決分析 ..... 47

第二節　我國法院判決差異分析 ..... 117

**第五章　結論與建議 ..... 125**

第一節　現行困境 ..... 125

第二節　對電商平台之建議 ..... 126

第三節　對法院與實務運作之建議 ..... 129

第四節　對法律修正之建議 ..... 133



doi:10.6342/NTU202501770

# 目次

**口試委員會審定書 ..... I**

**誌謝 ..... II**

**中文摘要 ..... IV**

**ABSTRACT ..... V**

**簡目 ..... VII**

**目次 ..... VIII**

**表次 ..... XVII**

**第一章　緒論 ..... 1**

第一節　研究背景與動機 ..... 1

一、　個資外洩事件頻發 ..... 1

二、　法律適用不確定性 ..... 2

三、　責任認定的複雜性 ..... 2

四、　國際法制比較的必要性 ..... 2

五、　企業面臨的挑戰 ..... 3

六、　研究的必要性和意義 ..... 3

第二節　研究目的 ..... 4

一、　明確法律責任與義務 ..... 4

二、　分析司法實務中的責任認定標準 ..... 4

三、　進行國際法規比較研究 ..... 4

第三節　研究方法 ..... 5

第一項　文獻分析法 ..... 5

第二項　歸納研究法 ..... 5



doi:10.6342/NTU202501770

第三項　比較研究法 ..... 5
第四節　研究架構 ..... 5
**第二章　歐盟一般資料保護規範（GDPR）下企業個資洩漏之責任 ..... 8**
第一節　GDPR 規定概述 ..... 8
第一項　GDPR 立法背景與目的 ..... 8
一、　立法背景 ..... 8
二、　GDPR 的核心目標 ..... 9
三、　GDPR 之影響 ..... 10
第二項　適用範圍與影響對象 ..... 11
一、　地域適用性（Article 3） ..... 11
二、　企業類型 ..... 12
三、　GDPR 的影響與企業應對策略 ..... 13
四、　小結 ..... 13
第二節　GDPR 核心原則與個人權利保障 ..... 13
第一項　GDPR 的核心原則（Article 5） ..... 13
一、　合法性、公正性與透明性（Lawfulness, Fairness, Transparency） ..... 13
二、　目的限制（Purpose Limitation） ..... 14
三、　資料最少化（Data Minimization） ..... 14
四、　準確性（Accuracy） ..... 14
五、　儲存限制（Storage Limitation） ..... 15
六、　完整性與機密性（Integrity and Confidentiality） ..... 15
七、　責任制與合規證明（Accountability） ..... 15
第二項　個人權利保障 ..... 15



doi:10.6342/NTU202501770

一、 存取權（Article 15）..... 15
二、 更正權（Article 16）..... 16
三、 刪除權（Article 17）或「被遺忘權」..... 16
四、 限制處理權（Article 18）..... 16
五、 資料可攜權（Article 20）..... 16
六、 異議權（Article 21）..... 16
第三節 GDPR 下損害賠償責任的認定與實務發展 ..... 17
第一項 GDPR 第 82 條的損害賠償規範 ..... 17
第二項 損害賠償範圍 ..... 17
一、 財產上損害（Material Damage）..... 17
二、 非財產上損害（Non-material Damage）..... 18
第三項 歐盟 GDPR 第 82 條實務發展 ..... 18
一、 CJEU C-300/21：政治傾向分析與非財產損害的認定 ..... 18
二、 CJEU C-667/21：內部健康資料洩漏與控制者過失推定 ..... 20
三、 CJEU C-340/21：駭客攻擊與控制者合規義務 ..... 21
四、 CJEU C-456/22：短暫資料公開與損害存在的舉證 ..... 23
五、 BGH VI ZR 10/24：失去資料控制即構成損害 ..... 25
六、 CJEU C-507/23：道歉作為補償的可行性 ..... 27
七、 CJEU C-182/22：身分資料外洩與懲罰性賠償排除 ..... 29
八、 判決比較分析 ..... 30
第四項 對企業責任制度的影響與制度反思 ..... 33
一、 企業法律義務之實質化與技術化 ..... 33
二、 訴訟風險之高度可預測性與風險外部化效應 ..... 33



doi:10.6342/NTU202501770

三、 制度設計上之反思與修正需求 ..... 34
四、 小結 ..... 34
**第三章 我國個資法規定與電商平台業者之個資管理義務 ..... 35**
第一節 個資法之立法背景與沿革 ..... 35
第一項 個資法之歷史背景 ..... 35
第二項 個資法歷次修法沿革 ..... 35
一、 2010 年修正 ..... 35
二、 2012 年施行 ..... 35
三、 2015 年修正 ..... 35
四、 2023 年修正 ..... 36
五、 個人資料保護委員會籌備處公告修正草案 ..... 36
第二節 個資法規範電商業者之個資管理義務 ..... 38
第一項 電商業者適用之法律範圍與基本原則 ..... 38
一、 合法性原則 ..... 38
二、 目的特定原則 ..... 38
三、 目的必要性原則 ..... 39
四、 資料正確性原則 ..... 39
五、 安全保障原則 ..... 39
六、 透明告知與當事人權利 ..... 39
第二項 個人資料之蒐集及告知義務 ..... 40
第三項 個人資料的處理與利用規範 ..... 40
第四項 資料安全管理與應變措施 ..... 40
第五項 委外處理與監督管理 ..... 41



doi:10.6342/NTU202501770

第三節　企業如何符合個資法第 27 條適當安全維護措施之標準 ..... 41
第一項　個資法第 27 條：安全措施與維護計畫 ..... 42
一、　立法背景與目的 ..... 42
二、　規範內容概述 ..... 42
三、　企業具體對應措施 ..... 43
第二項　個資法施行細則第 12 條：適當的安全措施 ..... 44
一、　立法背景與目的 ..... 44
二、　規範內容概述 ..... 44
三、　具體對應措施與實務應用 ..... 45
**第四章　我國個人資料外洩民事損害賠償責任之實務判決分析 ..... 47**
第一節　我國法院實務判決分析 ..... 47
第一項　橘熊科技股份有限公司（OB 嚴選）個資外洩案 ..... 47
一、　案件事實 ..... 47
二、　法院判決理由 ..... 48
三、　判決影響與未來發展之分析 ..... 50
第二項　雄獅旅行社股份有限公司 107 年個資外洩案 ..... 52
一、　案件事實 ..... 52
二、　法院判決理由 ..... 53
三、　判決影響與未來發展之分析 ..... 56
第三項　雄獅旅行社股份有限公司 108 年個資外洩案 ..... 58
一、　案件事實 ..... 58
二、　法院判決理由 ..... 59
三、　判決影響與未來發展之分析 ..... 60



doi:10.6342/NTU202501770

第四項　王品瘋美食 App 個資外洩案 ..... 62
一、　案件事實 ..... 62
二、　法院判決理由 ..... 64
三、　判決影響與未來發展之分析 ..... 68
第五項　北投麗禧溫泉酒店股份有限公司個資外洩案 ..... 70
一、　案件事實 ..... 70
二、　法院判決理由 ..... 72
三、　判決影響與未來發展之分析 ..... 75
第六項　中華民國運動神經元疾病友協會個資外洩案 ..... 77
一、　案件事實 ..... 77
二、　法院判決理由 ..... 79
三、　判決影響與未來發展之分析 ..... 81
第七項　威尼斯國際事業股份有限公司個資外洩案 ..... 83
一、　案件事實 ..... 83
二、　法院判決理由分析 ..... 84
三、　判決影響與未來發展之分析 ..... 88
第八項　迪卡儂個資外洩案 ..... 90
一、　案件事實 ..... 91
二、　法院判決理由 ..... 91
三、　判決影響與未來發展之分析 ..... 95
第九項　和雲行動服務股份有限公司 iRent 個資外洩案 ..... 97
一、　案件事實 ..... 97
二、　法院判決理由分析 ..... 98



doi:10.6342/NTU202501770

三、 判決影響與未來發展之分析 ..... 101
第十項 神腦國際企業有限公司個資外洩案 ..... 103
一、 案件事實 ..... 103
二、 法院判決理由分析 ..... 105
三、 判決影響與未來發展之分析 ..... 106
第十一項 三商行股份有限公司個資外洩案 ..... 108
一、 案件事實 ..... 108
二、 法院判決理由 ..... 109
三、 判決影響與未來發展之分析 ..... 111
第十二項 統聯汽車客運股份有限公司個資外洩案 ..... 112
一、 案件事實 ..... 113
二、 法院判決理由 ..... 114
三、 判決影響與未來發展之分析 ..... 115
第二節 我國法院判決差異分析 ..... 117
第一項 判決差異概述 ..... 117
第二項 法院主要認定準則 ..... 119
一、 侵權行為成立要件 ..... 119
二、 過失責任與違法性 ..... 120
三、 相當因果關係的認定 ..... 120
四、 舉證責任分配 ..... 120
第三項 因果關係與舉證責任 ..... 120
一、 因果關係的認定問題 ..... 120
二、 舉證責任分配的爭議 ..... 121



doi:10.6342/NTU202501770

三、 舉證困難與專家鑑定 ..... 122
第四項 企業安全維護義務與通知補救 ..... 122
一、 企業安全措施的審查 ..... 122
二、 事故發生後的通知義務與補救措施 ..... 123
三、 案件事實對賠償計算的影響 ..... 123
第五項 損害賠償範圍與計算 ..... 123
一、 損害賠償金額認定標準 ..... 123
二、 消費者自身責任的影響 ..... 123
三、 案件事實對賠償計算的影響 ..... 124
四、 第三人介入與消費者自身責任考量 ..... 124
**第五章 結論與建議 ..... 125**
第一節 現行困境 ..... 125
第二節 對電商平台之建議 ..... 126
一、 強化資安防護機制與標準化建置 ..... 126
二、 完備事故通報流程與證據保存紀錄 ..... 127
三、 重視消費者救濟與應變支持 ..... 127
四、 建立內部個資保護治理架構與人員培訓 ..... 128
五、 導入法律與保險工具分散風險 ..... 128
第三節 對法院與實務運作之建議 ..... 129
一、 強化舉證責任轉換與推定機制，落實個資法第 29 條保護目的 .... 130
二、 建立可操作之外洩來源推定標準，降低認定分歧 ..... 131
三、 參酌國際標準與政策準則，統一資安義務之審查依據 ..... 131
四、 明確法院對行政機關認定之處理原則，促進司法與行政一致性 .. 132



doi:10.6342/NTU202501770

五、 建立司法—行政—產業三方對話機制，提升專業判斷與制度整合 132

第四節 對法律修正之建議 ..... 133

一、 建立「明確化」的適當安全維護標準，提高業者可預期性 ..... 133

二、 引進資料保護影響評估與資料保護長制度，強化預防式治理機制 133

三、 強化個資事故通報義務，保障消費者即時反應權益 ..... 134

四、 補強民事損害賠償制度，明定損害類型與因果關係舉證準則 ..... 134

五、 健全主管機關功能，落實獨立監理與跨部會協調機制 ..... 135

**參考文獻 ..... 136**



doi:10.6342/NTU202501770

# 表次

【表 1】 GDPR 判決比較表 ..... 30

【表 2】 我國法院判決比較表 ..... 118



doi:10.6342/NTU202501770

# 第一章　緒論

## 第一節　研究背景與動機

近年來，隨著數位化時代的快速發展，個人資料已成為企業及平台業者運營的重要資產。然而，伴隨科技進步的同時，個資外洩事件層出不窮，導致詐騙案件頻繁發生，進一步引發民眾對於個人資料保護的憂慮。尤其是近來多起因個資外洩而導致的詐騙案，使得民眾財產損失慘重，引起社會廣泛關注。

一、個資外洩事件頻發

西元 2023 年臺灣多家企業接連爆發大規模個資外洩事件，導致數十萬名消費者的個資遭駭客竊取並被不法集團利用。例如，微風百貨遭駭客勒索，90 萬名會員的個資、訂單及付款資料等敏感資訊可能外流[1]、[2]；而 iRent 共享汽機車平台則因暫存資料庫防護漏洞，導致至少 40 萬名用戶的身分證、手機號碼及信用卡資訊面臨風險[3]。此外，刑事局指出部分電商平台資料庫遭駭，歹徒利用「解除分期付款」等詐騙手法，冒充客服人員騙取民眾的銀行資訊並要求操作 ATM 匯款，造成重大經濟損失[4]。這些事件暴露了企業在個資保護方面的漏洞，也凸顯了個資外洩對消費者造成的直接危害。面對此類案件，主管機關紛紛要求業者負起更高的個資管理責任，並加強行政檢查與裁罰，以確保個資保護機制的有效落實，同時，各企業紛紛採取措施強化資安防護，例如進行系統弱點掃描、加密交易過程及委請專業

---

[1] 數位時代〈微風個資外洩，經濟部、數發部組調查小組要查！誰讓 90 萬會員個資曝風險？〉，https://www.bnext.com.tw/article/74218/breeze-mall-hack?

[2] 經濟部〈經濟部對微風集團發生個資外洩事件之調查說明〉，https://www.moea.gov.tw/MNS/populace/news/News.aspx?kind=1&menu_id=40&news_id=105735

[3] 今周刊〈和泰旗下 iRent 爆個資外洩，公司道歉了…14 萬用戶擴大認定 40 萬，賠償方案「這天」出爐〉，https://www.businesstoday.com.tw/article/category/183027/post/202302020015/

[4] 內政部警政署刑事警察局〈公布 113 年第四季高風險業者排名 提醒消費者慎防詐騙〉，https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1887&serno=99151900-b8cb-4b95-bc5c-f3b0e8b51f94



doi:10.6342/NTU202501770

資安公司監控資料流出情形。然而，對於企業而言，應當做到何種程度才能算是符合個人資料保護法（以下簡稱個資法）的要求，並符合適當安全維護措施，仍然是一個值得深入探討的法律議題。

二、法律適用不確定性

目前法院針對個資外洩案件已有多起判決，但這些判決的差異顯示，在認定業者責任時，仍存在不同標準與見解。例如，某案例中，法院認定業者未盡妥善保護義務，須負擔民事損害賠償責任，但也有案例認為業者已經採取合理的安全防護措施，因此不應負擔全部責任。從法律角度而言，個資法要求業者必須採取「適當安全維護措施」，以保護個人資料免於洩漏、竄改、毀損、滅失或竊取。然而，「適當」的標準究竟如何界定，尚無明確的法律定義，而法院的判斷標準亦有所不同。這使得業者在實務運作中，對於個資保護措施的設置與維護，往往面臨不確定性的挑戰。

三、責任認定的複雜性

在判斷業者是否應負擔民事損害賠償責任時，需要考量多個因素，例如業者的安全措施是否符合業界標準、是否有足夠的風險評估機制、是否在個資外洩後迅速採取補救措施等。這些都是法律適用上的關鍵問題，需要深入探討和分析。在現行法律制度下，若業者未能適當保護個資，致使個人資料遭到洩漏，導致消費者受騙並遭受財產損失，則業者可能需依據民法第 184 條侵權行為責任規定，承擔損害賠償責任。此外，若業者未符合個資法所要求的「適當安全維護措施」，則可能違反個資法第 27 條，遭受主管機關裁罰，甚至衍生連帶的民事賠償責任。然而，若業者已採取合理的防護措施，但仍因駭客攻擊等不可抗力因素導致個資外洩，則其是否仍應負擔法律責任，亦值得進一步探討。這種情況下，如何平衡業者的責任與消費者的權益保護，成為一個重要的法律問題。

四、國際法制比較的必要性

從國際法制比較的角度來看，歐盟於西元（下同）2016 年制定並於 2018 年施行的一般資料保護規則（General Data Protection Regulation）對於個資保護標準與罰則有更為嚴格的規範，例如規定業者須確保「適當的技術和組織措施」，並對違反規定的業者施以高額罰款。相較之下，臺灣的個資法雖有相關規範，但對於「適



doi:10.6342/NTU202501770

當安全維護措施」的要求較為模糊，導致實務上對於業者責任的認定產生不同解釋。這種法規差異不僅影響了跨國企業的經營策略，也為臺灣的法制發展提供了參考方向。因此，透過比較研究，可以幫助我們更好地理解國際趨勢，並為臺灣的個資保護法制提供改進建議。

五、企業面臨的挑戰

隨著網際網路技術的不斷進步與電商模式的迅速普及，消費者對隱私權保護的重視程度日益提高，這不僅促使政府及監管機構加強相關法規建構，同時也使得企業在資料管理上面臨更高要求和更複雜的挑戰。企業需要在提供便利服務和保護用戶隱私之間取得平衡。一方面，他們需要收集和處理大量個人資料以優化用戶體驗和提供個性化服務；另一方面，他們必須確保這些資料的安全性，防止未經授權的訪問和濫用。此外，隨著資訊技術的快速發展，新型態的網路攻擊和資料竊取手段不斷出現，企業需要持續更新和升級其安全系統，以應對這些新興威脅。這不僅需要大量的技術投資，還需要建立完善的風險管理機制和應急預案。

六、研究的必要性和意義

鑑於上述背景和挑戰，深入探討現行法律框架下企業應承擔的賠償責任，不僅有助於減少未來可能發生的法律爭議，亦能夠在維護企業品牌形象、增強市場信心及促進公平競爭方面發揮積極作用。本研究的開展將有助於：

(一)明確在個資保護方面的法律義務和責任範圍，幫助業者更好地理解和遵守相關法規。

(二)通過分析實際案例，為業者提供實務指引，幫助他們在面對個資外洩事件時做出正確的應對。

(三)借鑒國際經驗，為臺灣的個資保護法制發展提供參考和建議。

(四)提出具體的風險管理策略，幫助電商業者建立更完善的個資保護機制，降低法律風險和經濟損失。

綜上所述，本研究旨在為電商業者、主管機關和立法者提供有價值的參考，以促進電子商務產業的健康發展，同時確保消費者的隱私權得到充分保護。



doi:10.6342/NTU202501770

## 第二節　研究目的

本研究的主要目的在於探討電子商務業者在個人資料外洩事件中所涉及的民事損害賠償責任，旨在協助業者更全面理解其在法律義務與風險上的定位，從而能夠建立並有效管理個人資料保護政策。隨著網際網路技術的不斷進步與電商模式的迅速普及，消費者對隱私權保護的重視程度日益提高，這不僅促使政府及監管機構加強相關法規建構，同時也使得業者在資料管理上面臨更高要求和更複雜的挑戰。

一、明確法律責任與義務

本研究首要目的是明確界定電商業者在個資保護方面的法律責任與義務。通過深入分析現行的個資法及相關法規，本研究將詳細闡述業者在資料蒐集、處理、儲存及傳輸過程中應遵守的安全管理標準與防範措施。這不僅包括對現有法律條文的解讀，還將結合實務案例，探討法院在判決中對這些義務的具體解釋和適用。

通過此分析，本研究旨在為電商業者提供一個清晰的法律框架，幫助他們更好地理解自身的責任範圍，從而採取更有針對性的措施來保護用戶個資。同時，這也將有助於業者在面臨個資外洩事件時，能夠準確評估自身的法律風險，並做出適當的應對。

二、分析司法實務中的責任認定標準

本研究的第二個重要目的是通過對國內法院判決案例的深入剖析，探討在個資外洩事件中，法院如何認定電商業者的過失責任及賠償額度。這一部分將重點關注判決中對「過失認定」、「因果關係」及「損害賠償範圍」等核心問題的認定標準。通過系統性地分析這些案例，本研究旨在歸納出法院在處理個資外洩案件時的主要考量因素和判斷標準。這將為電商業者提供寶貴的實務指引，幫助他們在日常運營中更好地評估和管理法律風險，並在面臨類似法律爭議時做出更有效的應對。

三、進行國際法規比較研究

鑒於全球個資保護法制的發展呈現多元化趨勢，本研究的第三個目的是進行國際法規比較研究。重點將放在比較 GDPR 之規範，探討其在處理個資外洩及賠償責任認定方面的制度設計與實務經驗。



doi:10.6342/NTU202501770

## 第三節　研究方法

### 第一項 文獻分析法

首先，收集並分析與個資外洩及民事賠償責任相關的學術文獻、法律條文、法院判決以及政府機構發布的報告。藉此掌握國內外電商平台在個資保護上的法律規範與實務操作，並深入理解現行法律在處理個資外洩事件中的適用情況。

### 第二項 歸納研究法

針對電商平台個資外洩的案例，從中歸納出導致個資外洩的常見原因與影響，並分析各個案例中民事賠償責任的判決依據與賠償範圍。透過歸納分析不同案例的共通性，逐步建立出有關電商業者個資外洩民事賠償的模式，以提供實務上的參考。

### 第三項 比較研究法

選取不同國家或地區對於電商平台個資外洩事件的法律規範及賠償責任進行比較，特別是對比各國在賠償責任認定、賠償範圍及法律責任的異同。此方法有助於瞭解國際間的法制發展，並找出我國電商平台在個資保護法規上可以參考與改進的方向，為電商業者制定更完善的風險管理策略提供基礎。

## 第四節　研究架構

本研究旨在探討電子商務平台業者於個人資料外洩事件中所應負擔之民事損害賠償責任，透過國內外相關法規、理論架構及實務判例的全面分析，具體釐清業者應負之法律義務與責任邊界，並提出制度調整與實務應對之具體建議。為使研究內容更具邏輯性與條理性，並協助讀者清楚掌握論文脈絡與分析方向，全文依研究主題與方法分為五章，其內容安排如下：

第一章　緒論

本章為全文之開端，主要說明研究背景與動機、研究目的、研究方法與研究範圍，並交代研究的重要性與價值。首先，本章說明在數位化與電商蓬勃發展的背景下，個資外洩事件層出不窮，不僅對消費者權益造成重大衝擊，也對企業信譽與法



doi:10.6342/NTU202501770

律責任產生深遠影響。在法規規範尚不明確、法院見解分歧之情況下，研究電商平台之法律義務與責任認定，有其迫切性與實務價值。其次，本章闡述研究方法，包括文獻分析法、歸納研究法與比較法等，說明如何透過理論與實務並重的方式進行探討。最後，也說明本研究之架構與章節安排。

第二章　歐盟一般資料保護規範（GDPR）下企業個資洩漏之責任

本章從國際比較法視角切入，詳細分析歐盟 GDPR 規範下關於個人資料外洩時企業責任之規定，尤其聚焦於第 82 條關於損害賠償的條文內容與判例詮釋。章節中依據歐洲聯盟法院（Court of Justice of the European Union，以下簡稱 CJEU）實務判決，探討在過失認定、資料來源追溯、舉證責任配置、因果關係評價與損害計算等面向之理論與實務發展，並評析其對我國法制建構的啟示。

第三章　我國個資法規定與電商平台業者之個資管理義務

本章回歸我國法律制度，聚焦於「個人資料保護法」對電商平台業者的規範。內容涵蓋個資法之立法沿革、核心義務與實務運作重點，包括資料蒐集、處理、利用之合法性要求，以及業者應採取之「適當安全維護措施」。同時說明 2023 年個資法修正之重點，例如強化罰則、通報機制、設立個資保護長制度等，說明政府如何透過立法回應社會對資安事故與業者責任的期待。最後，本章分析個資法第 27 條及施行細則第 12 條對「適當安全措施」的具體要求，作為後續企業責任判斷的基礎。

第四章　個資外洩之民事損害賠償責任分析

本章為論文的實證重心，彙整我國法院針對電商平台個資外洩民事訴訟之重要判決案例十二則，透過逐案分析法院對業者是否盡到資安維護義務、是否構成過失、資料外洩與損害之因果關係、損害範圍及非財產損害認定等方面的判斷標準與推理過程，歸納司法實務上之共通趨勢與解釋歧異。此章不僅揭示法院認定邏輯與標準之不一致性，也說明實務運作中所衍生之合規風險與證據困境。

第五章　結論與建議

本章綜整全篇研究成果，回應研究問題與目的。首先評析現行法律與司法實務在處理個資外洩事件責任歸屬上所面臨之制度困境與實務挑戰；其次提出針對電



doi:10.6342/NTU202501770

商業者在資訊安全建置、應變通報與證據保存等方面之具體實務建議；而後，就法院應建立一致性舉證標準、明確推定外洩來源機制與強化與行政認定間之互動，提出實務操作面建議；最後，呼籲立法機關應參考 GDPR 責任體系與國際發展趨勢，對我國個資保護法進行必要之修正與細化，建立清晰、可預期且可操作之法律框架，兼顧數位經濟發展與消費者隱私權益保障。



doi:10.6342/NTU202501770

# 第二章　歐盟一般資料保護規範（GDPR）下企業個資洩漏之責任

## 第一節　GDPR 規定概述

### 第一項 GDPR 立法背景與目的

一、立法背景

歐盟於 2018 年 5 月 25 日正式施行一般資料保護規則（General Data Protection Regulation，以下簡稱 GDPR），以取代 1995 年的資料保護指令（Data Protection Directive 95/46/EC）[5]。這項法規是全球最全面的數據保護法之一，旨在提升個人資料保護水準，並應對日益數位化社會所帶來的挑戰。由於數據科技的進步與互聯網的普及，企業能夠蒐集、儲存和分析大量個人數據，使得個人隱私面臨更高的風險。GDPR 的立法背景可以追溯至歐盟對數據隱私權的高度重視，並在技術發展與數據跨境流動的背景下，強化對個人資料的監管與保護。

GDPR 的適用範圍廣泛，不僅適用於歐盟境內企業，也適用於所有處理歐盟公民個人資料的機構，即便其企業總部位於歐盟境外。因此，無論是歐盟內部的企業，或是向歐盟公民提供商品或服務的國際企業，都必須符合 GDPR 的規範[6]。這種廣泛適用性的規定，使 GDPR 成為全球數據保護的標竿，並促使其他國家與地區，如美國加州的消費者隱私法（CCPA）[7]、[8]與中國的個人信息保護法（PIPL）

---

[5] Council of the European Union, “General Data Protection Regulation （GDPR)”, *Consilium*, https://www.consilium.europa.eu/en/policies/data-protection-regulation/ （last visited Apr. 7, 2025).

[6] activeMind.legal, “When Does the GDPR Apply to Non-EU Businesses?”, *activeMind.legal*, https://www.activemind.legal/guides/gdpr-non-eu-businesses/ （last visited Apr. 7, 2025).

[7] Palo Alto Networks, “What Is the California Consumer Privacy Act （CCPA)?”, Palo Alto Networks Cyberpedia, https://www.paloaltonetworks.com/cyberpedia/ccpa （last visited Apr. 7, 2025).

[8] IBM, “What Is CCPA?”, IBM Think, https://www.ibm.com/think/topics/ccpa-compliance （last visited Apr. 7, 2025).



doi:10.6342/NTU202501770

[9]，紛紛制定類似的法規。

二、GDPR 的核心目標

(一) 強化個人資料保護權利：GDPR 透過一系列強化個人權利的規定，使個資當事人（Data Subject）擁有更大的控制權。例如，個資當事人擁有「被遺忘權」（Right to be Forgotten），可要求企業刪除其個人資料，並擁有「資料可攜權」（Data Portability），允許個人將其個資轉移至其他服務提供者。此外，個資當事人還有權要求企業提供關於其個人數據的存取權限，確保透明度[10]。

(二) 統一歐盟內部法規：在 GDPR 之前，各歐盟成員國的數據保護法規並不統一，導致企業在不同國家面臨不同的法律要求，增加了合規成本。GDPR 的制定與實施統一了歐盟範圍內的個資保護標準，使企業無論在法國、德國、義大利或其他成員國運營，都需遵循相同的數據保護規範。這不僅提升了個人資料保護的一致性，也降低了企業在跨國業務中的法律不確定性。

(三) 提高企業的責任義務：GDPR 強化了企業在個人資料保護方面的責任。企業不僅需確保數據的安全性，還需證明其已採取適當的技術與組織措施來保護個人資料。企業若未能遵守 GDPR，可能面臨高額罰款[11]、[12]。例如，違反 GDPR 核心原則的企業，最高可能被罰全球營收的 4% 或 2000 萬歐元（以較高者為準）[13]。此外，企業必須任命資料保護官（Data Protection Officer, DPO），

---

[9] Secure Privacy, "Protecting Your Personal Data: A Guide to China's Personal Information Protection Law （PIPL)", *Secure Privacy*, Nov. 16, 2023, https://secureprivacy.ai/blog/china-pipl-personal-information-protection-law （last visited Apr. 7, 2025).

[10] 依據「一般資料保護規則」（General Data Protection Regulation, GDPR）第 17 條規定，資料當事人有權要求刪除其個人資料（即「被遺忘權」）。

[11] 蔣哲宇（2019），《個人資料保護法下對電商業適當安全維護措施之行政檢查》，頁 19，東吳大學法律學系科技法律研究組碩士論文。

[12] 林秉輝（2022），《企業洩漏個人資料之責任－以 GDPR 為中心》，頁 76，中原大學財經法律學系碩士論文。

[13] General Data Protection Regulation, Art.83.



doi:10.6342/NTU202501770

負責監督個資保護合規性，並建立「資料保護影響評估（Data Protection Impact Assessment, DPIA）」機制，以評估其數據處理活動的風險[14]。

(四) 促進數據安全與隱私保護技術發展：GDPR 鼓勵企業採用隱私保護技術（Privacy by Design and by Default）[15]，確保在設計產品或服務時就將隱私保護納入考量。例如企業可使用加密技術（Encryption）、假名化技術（Pseudonymization）來降低個資風險此外，GDPR 要求企業在發生數據洩漏時，必須在 72 小時內通報監管機構[16]，並通知受影響的個資當事人[17]，以確保透明度。

三、GDPR 之影響

GDPR 的推動對全球企業帶來了重大影響，尤其是大型跨國企業如 Google、Facebook、Amazon 等，皆須投入大量資源以確保合規。此外，歐盟監管機構對違反 GDPR 的企業進行嚴格監管，例如 2021 年對 Amazon 開出的 7.46 億歐元罰款[18]，以及 2019 年對 Google 施加的 5000 萬歐元罰款[19]，皆顯示 GDPR 對企業帶來的法律與經濟風險。

GDPR 透過強化個人權利、統一法規、提高企業責任義務及促進數據安全技術發展，成功提升了歐盟境內的個資保護水準。企業在數據保護上的合規性已成為全球競爭的重要一環，未來隨著更多司法判例的出現，GDPR 的適用範圍與解釋將更加明確，並對全球數據保護法規的發展產生深遠影響。

---

[14] General Data Protection Regulation, Art.37.

[15] General Data Protection Regulation, Art.25.

[16] General Data Protection Regulation, Art.33 1.

[17] General Data Protection Regulation, Art.34 1.

[18] iThome（2021 年 7 月 30 日），〈亞馬遜違反 GDPR 被罰 7.46 億歐元，創史上最高金額〉，載於：https://www.ithome.com.tw/news/145975（最後瀏覽日：2025 年 5 月 1 日）。

[19] iThome（2019 年 1 月 22 日），〈Google 違反 GDPR 被法國重罰 5,000 萬歐元〉，載於：https://www.ithome.com.tw/news/128391（最後瀏覽日：2025 年 5 月 1 日）。



doi:10.6342/NTU202501770

## 第二項 適用範圍與影響對象

GDPR 適用範圍不僅限於歐盟境內的企業與組織，還擴展至全球範圍內涉及歐盟公民個資的機構。GDPR 的地域適用性廣泛，涵蓋以下幾種情境：

一、地域適用性（Article 3）[20]

(一) 在歐盟境內營運的企業與組織

任何在歐盟境內設立並運營的企業或組織，不論其主要業務對象是否為歐盟公民，只要其處理個人數據，即必須符合 GDPR 的規範。這意味著，即使企業的業務重心是針對非歐盟地區，例如美國、亞洲或其他市場，若企業的營運範圍涉及歐盟，其仍受 GDPR 約束。例如：一家設立於德國的軟體公司，其產品主要銷售給美國市場，仍需符合 GDPR，因其在歐盟境內運營。法國的一家旅遊網站，即便其業務專注於非洲市場，由於其服務在歐盟境內提供，也需遵循 GDPR 的要求。

(二) 企業不在歐盟但提供商品或服務給歐盟居民

GDPR 不僅適用於歐盟境內企業，還涵蓋所有提供商品或服務給歐盟居民的企業，即使這些企業的總部或營運據點位於歐盟以外。例如：一家美國的電商平台允許歐盟消費者購買其商品，並提供歐盟地區的配送服務，則該電商平台需要遵守 GDPR。一家亞洲的線上教育機構，如果其網站提供歐盟語言選項（如德語、法語），並允許歐盟用戶註冊及付款，即便該企業未在歐盟設立分公司，仍屬於 GDPR 規範的對象。值得注意的是，企業是否受 GDPR 約束的關鍵，在於其是否「明確」針對歐盟市場。例如，如果企業僅偶爾接收到來自歐盟的顧客訂單，且未有針對歐盟市場的特定行銷策略，則可能不受 GDPR 的強制約束。然而，一旦企業有專門針對歐盟市場的業務規劃（如提供歐元結算、針對歐盟消費者的廣告行銷等），就必須遵守 GDPR。

(三) 監控歐盟居民行為的企業

GDPR 也適用於在歐盟境外的企業，只要其有監控歐盟居民行為的行為，例如

[20] General Data Protection Regulation, Art.3.



doi:10.6342/NTU202501770

利用數據分析或追蹤技術來蒐集歐盟用戶的個人數據。這類企業通常包括：使用 Cookies 追蹤歐盟用戶行為的網站與應用程式。透過數據分析技術收集歐盟居民的個資，如瀏覽紀錄、點擊行為等。監測社群媒體上的歐盟用戶互動，例如使用 AI 技術分析歐盟用戶的貼文、評論及興趣。這意味著，即使企業的伺服器設於美國或亞洲，只要其透過技術手段收集並處理歐盟居民的數據，便需遵守 GDPR 的相關規定。

二、企業類型

GDPR 的影響範圍廣泛，涵蓋不同類型的企業，尤其是涉及個資處理的機構，主要分為以下兩類：

(一) 資料控管者（Data Controller）[21]

資料控管者是指負責決定個人數據處理目的與方式的企業或組織，通常包括：電子商務平台，例如 Amazon、eBay 等，負責收集用戶的購買紀錄、付款資訊、地址等個人數據。金融機構與銀行：負責管理客戶的財務數據，如信用卡資訊、貸款申請、個人存款等。社群媒體平台：例如 Facebook、Twitter，這些企業儲存與分析大量的使用者個資。這些機構在 GDPR 規範下，需確保其處理個資的合法性，並提供用戶數據權利，如存取權、刪除權等。

(二) 資料處理者（Data Processor）[22]

資料處理者是指代表資料控管者處理個資的企業或機構，這些機構不直接決定數據的使用方式，而是依照控管者的指示處理數據，例如：雲端服務提供商：如 AWS、Google Cloud，為企業儲存和處理個資。行銷分析公司：透過數據分析技術追蹤用戶行為，提供市場洞察。支付平台：例如 PayPal、Stripe，處理客戶的付款資訊與交易數據。在 GDPR 規範下，資料處理者也需確保其操作符合數據安全標準，並與資料控管者簽署數據處理協議（DPA, Data Processing Agreement）。

---

[21] General Data Protection Regulation, Recital 74.

[22] General Data Protection Regulation, Recital 81.



doi:10.6342/NTU202501770

三、GDPR 的影響與企業應對策略

GDPR 施行後，企業若未能遵守規範，可能面臨高額罰款。例如，Google 曾因違反 GDPR 而被罰款 5000 萬歐元。因此，企業應採取適當的應對策略，如：數據透明化：清楚告知用戶其數據如何被收集與使用。強化數據安全措施：加強數據加密、存取控制等技術，防止數據洩露。建立合規機制：指派資料保護官（DPO），確保企業內部符合 GDPR 規範。提供用戶數據權利：允許用戶存取、刪除或修改其個資。

四、小結

GDPR 是當今全球最嚴格的數據保護法規之一，其適用範圍涵蓋歐盟境內外，影響所有涉及歐盟居民個資的企業與機構。無論企業位於何處，只要涉及歐盟公民的數據處理，就必須符合 GDPR 的要求，否則可能面臨高額罰款與法律責任。面對 GDPR 的規範，企業應採取適當措施，以確保數據處理的合法性與安全性，進而降低法律風險並提升用戶信任度。

## 第二節　GDPR 核心原則與個人權利保障

### 第一項 GDPR 的核心原則（Article 5）[23]

GDPR 確立了七大核心原則，以確保企業或機構在蒐集、儲存、處理和傳輸個人數據時遵守高標準的隱私保護規範。這些原則旨在強化個資保護機制，提高透明度，並賦予個資當事人更多權利。這七大核心原則包括：

一、合法性、公正性與透明性（Lawfulness, Fairness, Transparency）[24]

(一) 合法性（Lawfulness）：資料處理必須符合合法依據，包括但不限於當事人同意、契約履行、法定義務、公共利益或企業的合法利益。企業不得在無正當理由的情況下處理個人資料。

[23] General Data Protection Regulation, Art.5.

[24] General Data Protection Regulation, Art.5（1）（a).General Data Protection Regulation, Recital 39.



doi:10.6342/NTU202501770

(二) 公正性（Fairness）：企業在處理個人數據時，不得濫用數據以造成不公平或歧視。例如，企業不得因個資當事人的種族、性別或健康狀況而做出不合理的決策。

(三) 透明性（Transparency）：企業需明確告知個資當事人其個資的處理方式，包括蒐集目的、存儲期限、可能的第三方共享資訊等。企業應透過易懂的隱私政策讓使用者清楚掌握其數據流向。

二、目的限制（Purpose Limitation）[25]

GDPR 規定，企業蒐集個資時必須有特定且明確的目的，且該目的須合法且不得超出最初聲明的用途。例如，一家電商平台若蒐集客戶的個資以完成購物交易，則不得擅自將該數據用於廣告行銷，除非已獲得客戶明確同意。若企業未經當事人許可改變個資用途，則構成違規。

三、資料最少化（Data Minimization）[26]

企業應僅蒐集完成特定目的所需的最少數據，不得過度要求個資當事人提供非必要資訊。例如，一間社交媒體公司若要求使用者註冊帳戶，則應僅蒐集基本的身份驗證資料，而不應強制要求提供家庭住址或財務資訊。此原則有助於減少數據外洩的風險，並確保企業不囤積無用的個資。

四、準確性（Accuracy）[27]

控管者必須確保個人數據的準確性，並允許當事人隨時更正其個資。例如，一家銀行應確保客戶的聯絡資訊是最新的，若客戶更換電話號碼或住址，應提供簡單的機制讓客戶更新資訊。若企業因錯誤數據導致客戶遭受不利影響（如信用評分誤判），可能面臨法律責任。

---

[25] General Data Protection Regulation, Art. 5（1）（b).

[26] General Data Protection Regulation, Art. 5（1）（c).

[27] General Data Protection Regulation, Art. 5（1）（d).



doi:10.6342/NTU202501770

五、儲存限制（Storage Limitation）[28]

個資不得保存超過必要期限，企業需制定明確的數據刪除政策，確保資料在不再需要時及時刪除。例如，一家線上訂票系統應在客戶旅程結束後的合理期間內刪除其個人資料，而非無限期存儲。若數據因法定義務需長期保存（如醫療記錄），企業應確保其存儲方式符合安全標準。

六、完整性與機密性（Integrity and Confidentiality）[29]

企業須確保個資的安全性，防止未經授權存取、洩露或損毀。且企業應採取安全技術，如加密、存取控制和網路安全機制，以保護數據。例如，醫療機構在存儲病患資訊時，應確保其系統具備強大的存取權限管理，防止未經授權的人員存取敏感數據。

七、責任制與合規證明（Accountability）[30]

企業應證明自身符合 GDPR，包括內部政策、風險評估報告、數據處理紀錄等。企業可設置資料保護官（DPO），負責確保 GDPR 合規性。若發生數據外洩，企業需在 72 小時內通報監管機構，並通知受影響的個資當事人。

## 第二項 個人權利保障

GDPR 提供個資當事人多項權利，以確保其能有效控制自身數據。

一、存取權（Article 15）[31]

個資當事人有權要求企業提供其個人資料的存取權限，企業應提供一份可讀性高的數據副本。例如，一名社交媒體用戶可要求平台提供其所有個資，包括發送的訊息、點擊記錄和上傳的內容。

---

[28] General Data Protection Regulation, Art. 5（1)（e).

[29] General Data Protection Regulation, Art. 5（1)（f).

[30] General Data Protection Regulation, Art. 5（2).

[31] General Data Protection Regulation, Art. 15.



doi:10.6342/NTU202501770

二、更正權（Article 16）[32]

當事人有權請求企業更正其錯誤或過時的數據。例如，銀行應允許客戶隨時更新其地址資訊，以確保通訊的準確性。

三、刪除權（Article 17）[33]或「被遺忘權」

當事人可請求刪除其個資，例如數據已不再需要、當事人撤回同意或數據處理違反 GDPR 時。例如，一名使用者可要求社交平台刪除其多年未使用的帳戶及所有相關數據。

四、限制處理權（Article 18）[34]

當數據準確性或合法性存疑時，當事人可請求企業暫停處理其個資。例如，一名銀行客戶若對信用紀錄存疑，可要求暫停數據使用，直到爭議解決。

五、資料可攜權（Article 20）[35]

個資當事人可請求企業提供機器可讀格式的數據，以便轉移至其他服務供應商。例如，一名音樂串流服務用戶可要求平台提供其播放記錄，以便轉移至其他平台。

六、異議權（Article 21）[36]

當事人可拒絕企業處理其數據，尤其是用於行銷目的時。例如，一名消費者可選擇拒絕接收企業的行銷郵件。

透過七大核心原則與個人權利保障，確保個資的透明性、安全性與合規性。企業在蒐集、儲存與處理個人資料時，應確保符合這些規範，以避免潛在的法律責任。透過完善的內部政策與技術措施，企業能夠提升個資保護水準，並強化消費者對品

---

[32] General Data Protection Regulation, Art. 16.

[33] General Data Protection Regulation, Art. 17.

[34] General Data Protection Regulation, Art. 18.

[35] General Data Protection Regulation, Art. 20.

[36] General Data Protection Regulation, Art. 21.



doi:10.6342/NTU202501770

牌的信任感。

## 第三節　GDPR 下損害賠償責任的認定與實務發展

### 第一項 GDPR 第 82 條的損害賠償規範

GDPR 第 82 條明確規定，若企業或組織違反 GDPR 規範，導致個人資料外洩、不當處理或其他違規行為，進而使資料主體（data subject）遭受損害，該個人有權向控管者（controller）或處理者（processor）請求賠償（GDPR, Art. 82, 2016）。此條款的立法目的在於確保個人資料的基本權益獲得保障，並賦予個人有效的法律救濟手段，以應對企業不當處理個人資料所帶來的風險（European Commission, 2021）[37]。

### 第二項 損害賠償範圍

據 GDPR 第 82 條規定，凡因資料控制者或處理者違反本規則，而導致資料當事人受有損害者，當事人得向該控制者或處理者請求賠償。此條文所稱「損害」（damage）之範圍，並不僅限於傳統意義上的財產損失或金錢損害，而係採取一種開放且動態的理解，旨在回應數位社會中個人資料濫用所可能衍生之多元損害樣態。依據 GDPR 的立法目的與 CJEU 對第 82 條的解釋，損害大致可分為財產上財產上損害（material damage）與非財產上損害（non-material damage）兩大類型。

一、財產上損害（Material Damage）

財產上損害主要指可具體量化並具經濟性之損失，通常具有可核算之財務後果。例如，最常見者為個資外洩導致銀行帳戶或信用卡資料遭盜用，進而產生之金錢損失。此外，若因資料濫用而導致身份遭冒用、信用評分下降、貸款申請受阻、保險費率上升，亦屬間接財務損害。再者，資料當事人為防堵損害擴大，可能需支出法律費用、更換帳戶或購買保全服務，此類應對外洩風險所衍生之支出，亦構成可請求賠償之修復性成本。若外洩事件進一步導致商業合作喪失、職務流失等收入損失，亦應涵納於財產上損害範疇之內。

---

[37] General Data Protection Regulation, Art. 82.



doi:10.6342/NTU202501770

二、非財產上損害（Non-material Damage）

GDPR 對於非財產上損害之保障更為重要，尤反映其對個人尊嚴與人格權保護之高度重視。非財產上損害泛指無法以直接經濟方式加以量化，但對當事人權益已造成實質影響之損害。常見者包括：因擔憂資料被濫用所產生之焦慮、恐懼與精神壓力；因隱私資訊外洩（如健康、性傾向、宗教信仰等）而導致之名譽受損或社會排擠；以及對資訊控制權的喪失，即當事人無法再有效掌握、管理自身個資流向所引發的不安感與無力感。值得注意者，非財產上損害無需證明後續實質濫用即成立，只要資料保護權已被侵害，且該侵害引發合理的心理或人格性不利益，即可構成可賠償之損害。

## 第三項 歐盟 GDPR 第 82 條實務發展

從 CJEU 與德國聯邦最高法院的重要判決出發，整理並分析七件代表性案例，聚焦於非財產損害的認定、舉證責任配置、賠償金額原則與補償方式，藉此觀察歐盟司法體系如何詮釋並具體化 GDPR 第 82 條之損害賠償機制。

一、CJEU C-300/21[38]：政治傾向分析與非財產損害的認定

(一) 案件事實摘要：自 2017 年起，奧地利郵政公司（Österreichische Post）運用演算法分析個人資料，藉此推測個體之政治傾向，並建立所謂「目標群體地址」以供政治性廣告行銷使用。然申請人未曾同意其個人資料為此用途而進行處理，認為該資料處理行為已侵害其個人資料權益，並造成非財產上損害，包含心理焦慮及對資料控制者之信任喪失，遂向奧地利國內法院提起損害賠償訴訟，請求賠償金額為 1,000 歐元。奧地利最高法院於訴訟過程中，針對 GDPR 第 82 條關於損害賠償之適用，向 CJEU 聲請就下列三項法律問題進行前置性解釋：其一，是否僅因違反 GDPR 規定，即當然產生損害賠償請求權？其二，

[38] “CJEU – C-300/21 – Österreichische Post （Non-material damage in connection with the processing of personal data),” GDPRhub, https://gdprhub.eu/index.php?title=CJEU_-_C-300%2F21_-_%C3%96sterreichische_Post_%28Non-material_damage_in_connection_with_the_processing_of_personal_data%29 （last accessed: 25/05/2025)。



doi:10.6342/NTU202501770

非財產上損害是否須達一定之嚴重程度始得請求賠償？其三，損害賠償金額應如何認定？

(二) 法院判決重點：CJEU 於 2023 年 5 月 4 日作成判決，明確釐清 GDPR 第 82 條損害賠償制度之適用要件。其主要見解如下：首先，法院認為，依 GDPR 第 82 條規定，損害賠償請求權之成立，須同時具備三要件：一、控制者違反 GDPR 規定；二、資料主體遭受損害（包括財產上損害與非財產上損害）；三、違規行為與損害間具有因果關係。是故，僅有 GDPR 規範之違反而無損害結果者，不生損害賠償之請求權。其次，關於非財產上損害之成立標準，法院明確指出，GDPR 第 82 條並未要求非財產上損害須達「嚴重」程度。凡心理壓力、焦慮、不安感、失控感或信任感喪失等精神上不利益，只要可證明其存在，即屬可受償之非財產損害。若成員國內法另設嚴重性門檻，將違反 GDPR 之直接適用與統一解釋原則。最後，關於損害賠償金額之計算標準，CJEU 指出，GDPR 並未明文規範損害計算公式或金額上限，應由各成員國依其國內民事損害賠償制度裁量，惟其判定仍須符合「有效且充分補償」之原則，並應避免轉化為懲罰性賠償（punitive damages），以確保 GDPR 賠償制度之補償性本質。

(三) 判決後續影響與實務意義：本案對歐盟境內有關個人資料侵權損害賠償實務具有高度參考價值，其所釐清之法律標準，對未來各國法院處理 GDPR 第 82 條案件產生深遠影響。其一，本案排除了「違規即賠償」之主張，強調須由原告證明實際損害之發生及其與違規行為間之因果關係，有助於抑制濫訴風險，確保訴訟資源之合理分配。其二，對於非財產上損害之認定，法院明文否定成員國得以損害「未達嚴重」為由駁回請求，改以「有無可證明損害」作為標準，強化了對資料主體精神利益之保障，亦符合資料保護權作為人格權構成部分之保障理念。其三，雖法院未統一損害賠償金額之計算方式，惟要求各國於裁量時仍應確保賠償具「實質補償」功能，避免形式性裁定，有助於提升救濟制度之實效性。其四，從企業責任角度觀之，該判決實質上強化企業在資料處理過程中之合規義務，企業應預見任何未經同意之個資運用均可能衍生可證明之損害，從而承擔賠償責任。此一見解將促使企業於資料蒐集、分析與利用階



doi:10.6342/NTU202501770

段強化內部程序，從源頭減少潛在法律風險[39]、[40]。

二、CJEU C-667/21[41]：內部健康資料洩漏與控制者過失推定

(一) 案件事實摘要：本案原告為德國健康保險機構之一名員工，主張其雇主在未經其同意之情形下，將其健康資料以「醫療服務提供者」而非「雇主」之身分進行處理，已構成對 GDPR 第 6 條所定個人資料處理合法性原則之違反。原告進一步聲稱，此一違法處理行為對其造成精神壓力與睡眠障礙，應屬 GDPR 第 82 條所稱之非財產上損害，並因此請求相應損害賠償。本案之核心法律爭點主要包括：1.GDPR 第 82 條損害賠償責任是否須以「過錯」為構成要件；2.非財產上損害之認定標準及其舉證責任分配；3.該條文所規定之賠償責任是否具有懲罰性功能。

(二) 法院判決重點：CJEU 於 2023 年 12 月 21 日就本案作出判決。就上述爭點提出如下意見：首先，關於賠償責任是否以過錯為要件，法院明確指出，GDPR 第 82 條之責任體系採「推定過錯」（presumed fault）模式。亦即，當控制者違反 GDPR 規定並造成損害時，原則上應承擔損害賠償責任，惟其得透過證明：損害與其行為間不存在因果關係，或其已盡合理注意義務、無故意或過失，以免除其責任。此一見解實質上將舉證責任部分轉移至控制者，有助於強化資料主體之權益保障，並促使資料處理者在實務運作中採取更嚴謹之合規措施。其次，就非財產上損害之認定標準，法院指出，GDPR 第 82 條所稱之「損害」涵蓋非財產損害，且不以損害達一定嚴重程度為前提。但資料主體仍須提出具

---

[39] Inside Privacy – Covington & Burling LLP （2023), CJEU Clarifies the GDPR's Right to Compensation, available at: https://www.insideprivacy.com/eu-data-protection/cjue-clarifies-the-gdprs-right-to-compensation/ （last accessed: 25/05/2025).

[40] Clyde & Co （2025), *Loss of control over personal data: Is that sufficient for GDPR compensation?*, available at: https://www.clydeco.com/en/insights/2025/02/loss-of-control-over-personal-data （last accessed: 25/05/2025).

[41] GDPRhub （2024), CJEU – C-667/21 – Krankenversicherung Nordrhein, available at: https://gdprhub.eu/index.php?title=CJEU_-_C-667%2F21_-_Krankenversicherung_Nordrhein （last accessed: 25/05/2025).



doi:10.6342/NTU202501770

體證據，證明損害與資料處理行為間具相當因果關係。換言之，倘若資料主體僅主張抽象之不安感，或無法證明資料實際遭濫用，則不構成可賠償之損害。反之，即使僅係短暫之心理不適，如能證明其與控制者之違法行為具直接關聯，亦得獲賠。最後，法院明確否定 GDPR 第 82 條具有懲罰性功能，認為該條所規範之損害賠償制度，僅屬補償性質。是故，賠償金額應以彌補資料主體之實際損失為限，並不得另作為懲罰控制者或產生嚇阻效果之手段。

(三) 判決後續影響與實務意義：其一，就控制者責任之認定而言，本案確認責任體系採推定過錯模式，使控制者須負擔舉證其已盡合理注意義務之責，於實務上將促使資料控制者強化內部治理機制與紀錄保存制度，以應對未來潛在爭訟風險。其二，就非財產上損害之賠償，CJEU 在本案中與其先前之判決（如 C-300/21 與 C-340/21 案）一致，均未設置損害程度之門檻，惟仍要求具體損害事實及其與違法行為間之因果關係。該見解在兼顧保障資料主體權益與避免濫訴之間取得相對平衡。其三，對於賠償功能之界定，CJEU 再次強調 GDPR 第 82 條之損害賠償不具懲罰性，此與美國法上懲罰性賠償制度形成對比，有助於確保歐洲個資法賠償機制維持補償為本之基本價值，亦對未來跨國訴訟與法制比較提供參考。整體而言，C-667/21 判決不僅進一步細化 GDPR 第 82 條之適用要件與舉證標準，亦與先前 CJEU 實務相互呼應，強化對資料主體權益之保護，並為歐盟成員國法院提供統一明確之法律適用指引[42]。

三、CJEU C-340/21[43]：駭客攻擊與控制者合規義務

(一) 案件事實摘要：2019 年 7 月，保加利亞國家稅務局（National Revenue Agency,

---

[42] Philippe Heinzke, Reemt Matthiesen, Julia Dreyer, "News from the CJEU on GDPR Compensation," CMS Law-Now, 26 August 2024, available at: https://cms-lawnow.com/en/ealerts/2024/01/news-from-the-cjeu-on-gdpr-compensation （last visited May 29, 2025）。

[43] CJEU, Judgment of 14 December 2023 – Case C-340/21, *VB v. Natsionalna agentsia za prihodite*（ECLI:EU:C:2023:986), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A62021CJ0340 （last accessed: 25/05/2025).



doi:10.6342/NTU202501770

NAP）遭遇大規模駭客攻擊，導致超過六百萬名納稅人之個人資料，包括稅務紀錄、社會保險資訊及其他高度敏感資料，遭非法存取並被揭露於網路上。受害人主張，NAP 作為 GDPR 下之資料控制者，未依據 GDPR 第 5 條、第 24 條及第 32 條規定，採取適當之技術與組織措施（Technical and Organisational Measures, TOMs），以確保個人資料之安全與保密性。原告進一步主張，因其個資外洩而產生對未來資料濫用之恐懼與焦慮，已構成 GDPR 第 82 條所稱之「非財產上損害」，據此請求賠償。第一審法院認為，NAP 已採取合理之資安措施，資料外洩係因第三方駭客之非法行為所致，故駁回原告請求。原告不服，提起上訴。爭點集中於：一、資料控制者能否以第三方非法攻擊為由，主張責任豁免；二、恐懼與焦慮是否構成 GDPR 下之非財產上損害；三、舉證責任應如何分配。

(二) 法院判決重點：

1. 資料控制者之責任界限：CJEU 就本案明確指出，GDPR 第 82 條第 3 項固然允許資料控制者主張「損害非其所致」以排除賠償責任，惟該項豁免條款須從嚴解釋。控制者若欲主張免責，須證明其已依 GDPR 第 24 條及第 32 條規定，對於處理個人資料之風險，採取所有適當之技術與組織措施，並且該損害之發生並非因其違反 GDPR 義務所致。換言之，僅以「第三方非法行為」為抗辯，尚不足以完全免除其法律責任。法院同時強調，控制者於訴訟中負有主動舉證責任，應提出具體證據以證明其已盡合理注意義務。

2. 非財產上損害之構成要件：關於非財產上損害之認定，法院認為，若因個資外洩而引發心理層面之恐懼或焦慮，且其情狀具備客觀事實基礎，則可構成 GDPR 第 82 條所稱之損害。惟原告仍負有舉證責任，須證明其確實因資料外洩遭受心理上之實際損害，而非僅憑資料外洩事實即推定損害之存在。法院進一步指出，損害賠償請求無需達特定「嚴重性」門檻，惟賠償僅限於「實際損害」，不得主張懲罰性賠償。

3. 適當技術與組織措施之評價標準：就控制者是否採取「適當措施」之判斷標準，法院指出，應綜合考量資料處理之性質、範圍、情境與目的，並衡酌資料主體權利可能受損之程度與嚴重性。控制者並應定期進行風險評估，並據以調整其



doi:10.6342/NTU202501770

TOMs。若控制者能證明其所採措施符合國際資訊安全標準(如 ISO/IEC 27001),將有助於舉證其已盡合理保護義務。

(三) 判決後續影響與實務意義：本案係 GDPR 施行以來，首宗涉及國家機關大規模資料外洩所引發之損害賠償案件，對歐盟境內資料保護實務產生深遠影響。其對企業與公部門控制者釐清以下幾項實務原則：第一，控制者有責任建立持續且可驗證之風險管理機制，並留存 TOMs 之設計與執行情形，以備未來於訴訟中作為合規證明之依據[44]。第二，對於主張非財產上損害賠償之原告而言，其主張須具備具體事實支持，並須證明心理損害與資料外洩事件間具因果關係。第三，本案亦可能推動資訊安全保險機制及主管機關對資料處理風險之監管標準，進一步強化控制者對資安與合規性之重視。綜上所述，CJEU 於 C-340/21 案所為之判決，進一步強化 GDPR「問責原則」(accountability principle)之落實，要求資料控制者於面對個資外洩事件時，應非僅止於形式上之合規，而須能具體證明其已採取充分且適切之防護措施[45]。

四、CJEU C-456/22[46]：短暫資料公開與損害存在的舉證

(一) 案件事實摘要：2020 年，德國地方政府 Gemeinde Ummendorf 於執行市政會議程序時，因行政疏失將一份包含兩名資料主體（VX 與 AT）全名及住址之議程文件，未經遮蔽即上傳至其官方網站，導致該等個人資料於網路上公開達數日之久。資料主體認為，此舉構成對其個人資料之不當處理，違反 GDPR 第

---

[44] Harneys Regulatory Blog, "CJEU Ruling Clarifies on Liability, Damages and TOMs for Data Breaches," Harneys, 19 April 2024, available at: https://www.harneys.com/our-blogs/regulatory/cjeu-ruling-clarifies-on-liability-damages-and-toms-for-data-breaches/（last visited May 29, 2025）。

[45] Arthur Cox （2024), Summary of 2023's Key CJEU Data Protection Judgments, available at: https://www.arthurcox.com/knowledge/summary-of-2023s-key-cjeu-data-protection-judgments/ （last accessed: 25/05/2025).

[46] GDPRhub （2024), CJEU – C-456/22 – Gemeinde Ummendorf, available at: https://gdprhub.eu/index.php?title=CJEU_-_C%E2%80%91456%2F22_-_Gemeinde_Ummendorf （last accessed: 25/05/2025).



doi:10.6342/NTU202501770

5 條第 1 項第 f 款所定「完整性與保密性原則」及第 32 條所規定之「適當安全措施義務」，遂依 GDPR 第 82 條向地方法院請求非財產上損害賠償。Gemeinde Ummendorf 則抗辯稱，該事件雖涉及個資外洩，惟涉案資料僅短暫公開，並未造成實質損害，請求法院採取「最低損害門檻」（de minimis threshold）之標準而駁回原告請求。德國 Ravensburg 地方法院於審理中遂向歐盟法院（CJEU）提請前置裁定，請求釐清 GDPR 第 82 條損害賠償適用上，非財產上損害是否需達「顯著程度」方得請求，以及資料控制者與資料主體間舉證責任之分配標準。

(二) 法院判決重點：歐盟法院於本案中，就 GDPR 第 82 條關於非財產上損害賠償之適用，提出若干重要見解，對既有成員國實務見解形成重大修正。

1. 首先，法院明確指出，GDPR 第 82 條並未賦予成員國裁量空間得設立請求損害賠償之「最低門檻」。資料主體只需證明：（1）資料控制者存在違反 GDPR 之行為；（2）資料主體確實受到損害，包括對個資失控所引發之焦慮或不安；（3）該損害與違法行為間具因果關係，則應准予損害賠償，無須證明損害具備「客觀顯著性」。此判斷實質推翻德國法院所採「顯著性門檻」理論，並統一歐盟區域內對非財產上損害之認定標準。

2. 其次，法院就舉證責任問題採取雙重標準。依據本案見解，資料主體須負舉證責任，證明其受有損害並與違法行為具因果關係，惟法院允許其得以「合理推論」（plausible inference）方式證明之，無需具體量化損害程度。反之，資料控制者則負有舉證責任，須證明其已採取 GDPR 第 32 條所要求之「適當技術與組織措施」（technical and organisational measures, TOMs），或損害並非因其行為所致。此舉顯著提高資料控制者於民事訴訟中之舉證義務強度。

3. 再者，法院亦對於賠償金額之計算原則加以釐清，重申 GDPR 損害賠償之核心目的在於補償（compensation），而非懲罰（punitive）。因此，不得因控制者主觀過失程度而提高賠償額度，亦不得就同一違法處理行為，重複計算其違反多項 GDPR 條文所生之損害。

(三) 判決後續影響與實務意義：CJEU 本案判決對於 GDPR 第 82 條的適用與解釋，具里程碑性意義，未來無論在企業實務或各成員國之司法實踐均將產生深遠



doi:10.6342/NTU202501770

影響。其一，就企業面言，此判決導致訴訟風險顯著升高。過往各國法院對於「輕微個資外洩」事件（如誤寄電子郵件）多採容忍態度，然本案所揭示之「低門檻損害理論」將使企業面對日益增多之小額求償案件。此外，因法院要求控制者須能證明資安措施符合風險水準，企業應強化內部資安治理體系，導入自動化個資檢測系統，或定期執行資安演練並建構完整 DPIA（Data Protection Impact Assessment）報告，以供舉證之用。其二，在法律解釋層面，本案有效統一各成員國對 GDPR 第 82 條之適用見解，特別是對德國「顯著性門檻」、奧地利「風險推定理論」、與荷蘭要求損害具體化之見解產生排除與統整作用（Conflict of Laws, 2024）。該等解釋趨勢有助於歐盟境內資料保護法律適用之一致性與可預測性。其三，未來司法實踐可望發展出「非財產上損害類型化」判準，例如：資料外洩之持續時間、資料敏感性、公開對象與範圍等均可能成為損害認定之具體指標。與此同時，企業亦需強化「合規文件化」之準備，例如內部資安政策、技術措施審查報告及應變演練紀錄，作為抗辯依據，以因應日益嚴格之合規審查與舉證壓力[47]、[48]。

五、BGH VI ZR 10/24[49]：失去資料控制即構成損害

(一) 案件事實摘要：本案係緣於 Meta Platforms Ireland Ltd.（原 Facebook）於 2019 年間所發生之一宗個人資料外洩事件。該事件係駭客透過平台應用程式介面（API）之技術漏洞，擷取大量用戶資料並將之非法公開。原告之手機號碼即因此遭揭露於網路空間，主張此一資料揭露侵害其個人資料控制權，乃依據 GDPR 第 82 條請求非財產損害賠償，並進一步聲請確認未來損害責任

---

[47] Matheson （2023), CJEU provides clarity on right to compensation for GDPR infringements, available at: https://www.matheson.com/insights/detail/cjeu-provides-clarity-on-right-to-compensation-for-gdpr-infringements （last accessed: 25/05/2025).

[48] Loyens & Loeff （2023), Legal Framework on Non-Material Damages under the GDPR: A Status Quo, available at: https://www.loyensloeff.com/insights/news--events/news/legal-framework-on-non-material-damages-under-the-gdpr-a-status-quo/ （last accessed: 25/05/2025).

[49] “BGH – VI ZR 10/24,” GDPRhub, available at: https://gdprhub.eu/index.php?title=BGH_-_VI_ZR_10%2F24 （last visited May 29, 2025）。



doi:10.6342/NTU202501770

（Feststellungsklage）及發出禁制令。本案之爭點主要包括：其一，單純喪失對個人資料之控制權，是否足以構成 GDPR 第 82 條所稱之「非財產損害」；其二，Facebook 預設開放用戶電話號碼供搜尋之設定，是否違反資料最小化原則及預設資料保護義務；其三，關於未來損害之確認請求，其在實體法上之合法性基礎為何；其四，損害之舉證責任與金額量化，應採何等標準加以認定。

(二) 法院判決重點：首先，法院明確採納 CJEU 於 C-300/21（Österreichische Post 案）中所揭示之見解，認為資料主體若因資料控制者之疏失而失去對個資之控制權，即構成 GDPR 第 82 條意義下之非財產損害。法院指出，在數位時代中，個人資料控制權係屬人格權保障之核心，資料控管者若未落實適當保護措施而致個資外洩，即屬對資料主體自主決定權之持續侵害，而該種「控制權喪失狀態」（Kontrollverlust），本身即足以構成可賠償之非財產損害，無須另證明具體心理創傷。其次，就平台預設開放電話號碼搜尋功能之合法性，法院認為違反 GDPR 第 5 條第 1 項第（c）款所定之資料最小化原則，並同時違反 GDPR 第 25 條第 2 項規定之「預設資料保護義務」（privacy by default）。法院指出，平台未能證明該項功能對服務提供具絕對必要性，亦未區分不同使用者情境即一律適用，違反風險導向之個資保護精神。最後，關於確認未來損害責任之請求，法院創設所謂「持續風險理論」（konkrete Gefahr），認為個資外洩所生之風險具長期性與擴散性，若原告得證明未來仍存有資料遭濫用之具體危險，即可主張確認請求權之正當利益，為個資侵害案件創建前所未有之救濟途徑。

(三) 判決後續影響與實務意義：本案判決不僅確立「控制權喪失即為損害」之新型非財產上損害認定標準，更彰顯 GDPR 風險責任架構之深化與發展，對歐陸各國法院未來處理類似案件具有重要指導意義。首先，在損害認定層面，原告無須再負擔舉證精神痛苦之高標準，訴訟門檻之降低將有助於促進個資保障訴訟之提起，並提高集體訴訟之可能性。德國亦因此成為歐盟內首個明確採納該標準之法院，與奧地利最高法院於 Schrems II 後續判決之態度互相呼應。其次，法院對 GDPR 第 25 條關於預設資料保護義務提出具體化操作標準，包括：1.處理必要性之實質檢驗；2.依用戶情境差異進行資料處理設定；3.對高敏感性資料採取最高保護層級之預設值。此對企業平台設計階段即強調合規性內建（compliance by design）與風險最小化策略，實有促進隱私工程發展之



doi:10.6342/NTU202501770

效果。再者，關於損害量化之方法，法院指示下級審應依德國民事訴訟法第 287 條，考量外洩資料敏感性、控管者之過失程度及侵害持續期間等因素，建立「階梯式賠償模型」，此與傳統慰撫金酌定機制不同，更能反映數位環境下侵害特性。最後，從政策意涵觀察，此判決展現歐洲司法實務對風險本位資料保護精神之擁抱，與美國加州消費者隱私法（CCPA）所強調之「實際損害」路線相異。該判決將進一步迫使企業於 API 控管、預設隱私模組與風險監測系統上加大投入。然而，亦有學者憂心該「準嚴格責任」模式對中小企業造成過重負擔，未來如何於維護個資權益與促進數位經濟間取得平衡，將成為後續立法與政策調整之核心課題[50]、[51]。

六、CJEU C-507/23[52]：道歉作為補償的可行性

(一) 案件事實摘要：本案發生於拉脫維亞，爭議主體為拉脫維亞消費者權益保護中心（以下簡稱 PTAC）與一名知名記者（資料主體）之間。PTAC 於一項宣導消費者認識二手車購買風險之活動中，製作並公開發佈宣傳影片，影片中角色明顯模仿並影射該名記者，且未經其同意即使用其個人形象與資料。資料主體認為此舉已損害其聲譽，構成非財產上損害，遂請求 PTAC 停止影片流通，公開道歉並支付 2,000 歐元作為損害賠償。PTAC 拒絕其請求後，資料主體向拉脫維亞地方法院提起訴訟。地方法院認定 PTAC 未經授權處理個資，違反 GDPR 規定，判命 PTAC 公開道歉並支付象徵性賠償金 100 歐元。PTAC 不服

---

[50] Clyde & Co, "The New Leading Decision Procedure of the Federal Court of Justice on Damages under the GDPR," Clyde & Co Insights, 22 November 2024, available at: https://www.clydeco.com/en/insights/2024/11/the-new-leading-decision-procedure-of-the-federal（last visited May 25, 2025）。

[51] DLA Piper Privacy Matters, "Germany: Judgment on Non-Material Damages for Loss of Control over Personal Data," Privacy Matters Blog, 22 November 2024, available at: https://privacymatters.dlapiper.com/2024/11/germany-judgment-on-non-material-damages-for-loss-of-control-over-personal-data/ （last visited May 29, 2025）。

[52] CJEU, Judgment of 14 December 2023 – C-456/22. Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=290709（last visited May 29, 2025）。



doi:10.6342/NTU202501770

提起上訴，二審法院確認 PTAC 違法，並命其於所有曾發佈影片之網站公開道歉，惟認為該行為係基於公共利益目的，且未造成嚴重損害，駁回金錢賠償部分請求。原告不服，進一步主張依 GDPR 第 82 條請求非財產上損害賠償，爭點包括：1.僅有 GDPR 違規是否足以構成「損害」？2.公開道歉是否足以完全補償非財產上損害？3.法院於計算賠償金額時，是否得斟酌控制者之主觀意圖與違規程度？拉脫維亞最高法院遂就相關法律適用疑義，向 CJEU 申請初步裁決。

(二) 法院判決重點：歐盟法院於 2024 年 10 月 4 日作出 C-507/23 號判決，針對 GDPR 第 82 條損害賠償之適用標準提出重要釐清。

1. 首先，法院明確採取「三要件累積原則」（Kumulationserfordernis），即須同時具備「違反 GDPR 之行為」、「資料主體遭受實際損害」，以及「行為與損害間具有因果關係」，方得成立損害賠償請求。

2. 其次，關於非財產損害之範圍，法院指出，名譽受損、精神痛苦等情形原則上得構成 GDPR 第 82 條所稱「非財產上損害」，惟須由原告具體證明損害之存在及其嚴重性，不能僅以資料處理違法即主張損害存在。

3. 再者，對於道歉是否可視為賠償方式，法院認為，在無法回復原狀之情形下，若誠懇且具補償效力，道歉得作為獨立或補充性之救濟措施，但應依個案具體情節判斷道歉之實質效果與充分性。

4. 最後，法院重申第 82 條之損害賠償制度為「補償性」，不具有懲罰性目的，故不得斟酌控制者之主觀惡意或違規程度，亦不應引入懲罰性賠償之概念。惟即使損害輕微，法院仍應保障資料主體之「完全賠償」（full compensation）權利，得酌定象徵性金額以資彌補。

(三) 判決後續影響與實務意義：CJEU 本案判決對於 GDPR 第 82 條損害賠償機制之適用具有深遠意義。就企業與資料控制者而言，該判決強化了事前合規作為之重要性，避免企業以道歉為事後補救策略；同時亦須重新檢視現行責任保險條款，評估涵蓋非金錢性補償形式之風險範圍。對司法實務而言，法院對於「損害」構成要件之明確界定，有助於減少濫訴與誇大主張之情形，並促使資料主體於訴訟中積極主張並舉證其遭受之非財產損害。另就賠償形式而言，該判決



doi:10.6342/NTU202501770

亦為各會員國法院於衡量公開道歉、聲明更正等多元補償方式提供一定裁量空間。從整體 GDPR 體系觀之，本判決強調第 82 條與第 83 條之功能區隔，一為補償性損害賠償規範，另一則為行政制裁條款，有助於釐清兩者之立法目的與適用準則，避免於司法適用上產生混淆[53]、[54]。

七、CJEU C-182/22[55]：身分資料外洩與懲罰性賠償排除

(一) 案件事實摘要：本案係發生於德國，原告於線上投資交易平台 Scalable Capital 開設帳戶時，需提供姓名、出生日期、住址、電子郵件等基本個人資料，並上傳身分證數位影本，另預付數千歐元作為開戶押金。惟在此程序中，申請人之個人資料遭不明第三方未經授權竊取。雖然事後並無證據顯示該等資料已被實際濫用於詐欺、盜領或其他違法用途，惟原告主張自身已因此遭遇精神壓力與焦慮等非財產損害，遂依 GDPR 第 82 條之規定向慕尼黑地方法院提起損害賠償之訴。本案遂涉及數項關鍵法律爭點，包括：其一，單純資料外洩而無實際濫用情形是否已構成損害；其二，非財產上損害是否需達特定嚴重程度始得請求賠償；其三，第 82 條所定損害賠償制度是否具有懲罰性質。

(二) 法院判決重點：CJEU 於本案中明確釐清 GDPR 第 82 條之適用要件與性質，認定資料主體為請求損害賠償，須符合三項構成要件：1.存在 GDPR 義務違反事實，即資料控制者未能履行其保護個人資料之實質義務；2.申請人確實遭受損害，且此處之「損害」包括財產上損害與非財產上損害，無須達到「重大性」

---

[53] Arthur Cox, "Summary of 2024's Key CJEU Data Protection Judgments," Arthur Cox Knowledge, 10 January 2025, available at: https://www.arthurcox.com/knowledge/summary-of-2024s-key-cjeu-data-protection-judgments/（last visited May 29, 2025）。

[54] DLA Piper Privacy Matters, "EU CJEU Insight: Key Takeaways from Recent Rulings on GDPR Damages," Privacy Matters Blog, 30 October 2024, available at: https://privacymatters.dlapiper.com/2024/10/eu-cjeu-insight/（last visited May 29, 2025）。

[55] "CJEU – C-182/22 and C-189/22 – Scalable Capital （Joined Cases)," GDPRhub, available at: https://gdprhub.eu/index.php?title=CJEU_-C%E2%80%91182%2F22_and_C%E2%80%91189%2F22-Scalable_Capital%28Joined_Cases%29（last visited May 29, 2025）。



doi:10.6342/NTU202501770

或「嚴重性」等門檻標準；3.違規行為與損害間存有相當因果關係，亦即若無該違規即不會發生損害，而不需證明單一違規行為為損害唯一原因。關於賠償制度之性質，法院進一步指出第 82 條之目的係為損害補償，排除懲罰性功能，強調該條文僅具補償（compensatory）性質，並非為懲罰控制者或產生威嚇效果。至於舉證責任部分，法院重申資料控制者有義務證明其已採取 GDPR 第 24 條及第 32 條所要求之適當技術與組織措施，否則即不得主張免責。

(三) 判決後續影響與實務意義：本案判決對 GDPR 實務適用產生數項重要影響。首先，在非財產上損害之認定上，CJEU 否定部分成員國法院主張之「最低嚴重性門檻」要求，意即即使損害僅表現為焦慮、不安或精神壓力等抽象感受，只要能具體舉證，即應認可其賠償請求，對資料主體權利形成有力保障。其次，該案強化資料控制者之合規義務與舉證責任，倘控制者無法證明其已履行適當安全措施，即須承擔賠償責任，形同形成一種「推定過失」機制，實務上勢將提升企業對資安防護之投資與訴訟防禦成本。再者，法院亦重申賠償金額計算應遵循「完全補償原則」，即補償實際所生損害為限，避免因同一資料外洩事件中涉多項違規行為而重複求償。整體觀之，本案實質強化資料主體保護機制，並為日後評價精神性損害、確認因果關係及賠償計算原則提供實務參照[56]。

八、判決比較分析

為全面理解 GDPR 第 82 條損害賠償制度之實務運作，本文整理歐洲法院（CJEU）及德國聯邦最高法院關於個人資料外洩事件中民事責任之代表性判決，彙整其於「過失推定」「非財產損害認定」「因果關係評價」等核心要素之判斷趨勢，以比較各案裁判重點。相關內容如【表 1】所示。

【表 1】 GDPR 判決比較表

[56] Timelex, “Recent CJEU Judgements Concerning the Right to Compensation under Art. 82 GDPR: State of Affairs in Ten Focus Points,” Timelex Blog, 26 February 2024, available at: https://www.timelex.eu/en/blog/recent-cjeu-judgements-concerning-right-compensation-under-art-82-gdpr-state-affairs-ten-focus（last visited May 29, 2025）。



doi:10.6342/NTU202501770

| 案例/判決 | 主要爭點/事實摘要 | 判決重點/實務影響 |
| --- | --- | --- |
| CJEU C-300/21<br>奧地利郵政利用演算法分析政治傾向，未經同意處理個資，導致心理焦慮與信任喪失 | 1. 損害賠償請求需符合三要件：違反GDPR、損害存在（包括非財產上損害）、違規行為與損害間具因果關係。<br>2. 非財產上損害不需達「嚴重程度」，心理壓力、焦慮等精神不利益即可構成損害。<br>3. 賠償金額由成員國裁量，但需符合「有效且充分補償」原則，避免懲罰性賠償。 | 1. 排除「違規即賠償」主張，抑制濫訴。<br>2. 強化資料主體精神利益保障。<br>3. 促使企業加強資料處理合規性。 |
| CJEU C-667/21<br>德國健康保險機構員工健康資料遭違法處理，造成精神壓力與睡眠障礙 | 1. GDPR 第 82 條採「推定過錯」模式，控制者需證明已盡合理注意義務以免責。<br>2. 非財產上損害不需達一定嚴重程度，但需證明損害與違法行為間具因果關係。<br>3. 賠償制度僅具補償性，排除懲罰性功能。 | 1. 強化控制者舉證責任，促進內部治理。<br>2. 平衡資料主體權益與濫訴風險。<br>3. 確保賠償制度的補償性本質。 |
| CJEU C-340/21<br>保加利亞稅務局遭駭客攻擊，導致個資外洩，原告主張恐懼與焦慮構成非財產上損害 | 1. 控制者若欲免責，需證明已採取 GDPR 要求的適當技術與組織措施。恐懼與焦慮可構成非財產上損害，但需具備客觀事實基礎。<br>2. 賠償金額僅限於實際損害，排除懲罰性賠償。 | 1. 強化控制者風險管理與資安措施。<br>2. 推動資訊安全保險與監管標準。<br>3. 確立「問責原則」的實務操作。 |



doi:10.6342/NTU202501770

| 案例/判決 | 主要爭點/事實摘要 | 判決重點/實務影響 |
| --- | --- | --- |
| CJEU C-456/22<br>德國地方政府短暫公開個資，原告請求非財產上損害賠償 | 1. GDPR 第 82 條不設最低損害門檻，資料主體只需證明損害存在及因果關係。<br>2. 控制者需舉證已採適當技術與組織措施。<br>3. 賠償金額計算應避免重複求償，僅補償實際損害。 | 1. 訴訟風險升高，企業需強化資安治理。<br>2. 統一歐盟內非財產上損害認定標準。<br>3. 推動「非財產上損害類型化」判準。 |
| BGH VI ZR 10/24<br>META（FACEBOOK）個資外洩，喪失資料控制權即構成損害 | 1. 單純喪失資料控制權即構成非財產損害。<br>2. 平台預設資料公開功能違反資料最小化原則與預設資料保護義務。<br>3. 創設「持續風險理論」，允許確認未來損害責任。 | 1. 降低資料主體舉證門檻，促進個資保障訴訟。<br>2. 強化平台設計階段的合規性內建。<br>3. 建立「階梯式賠償模型」以量化損害。 |
| CJEU C-507/23<br>拉脫維亞 PTAC 未經同意使用記者形象，造成名譽受損，請求道歉與賠償 | 1. 損害賠償需符合三要件：違規行為、損害存在、因果關係。<br>2. 道歉可作為補償方式，但需具備實質效果。<br>3. 賠償制度僅具補償性，排除懲罰性目的。 | 1. 強化事前合規重要性，避免企業僅以道歉為補救。<br>2. 減少濫訴，促進資料主體舉證。<br>3. 明確第 82 條與第 83 條功能區隔。 |
| CJEU C-182/22<br>德國線上投資平台個資外洩，無實際濫用，原告主張精神壓力與焦慮 | 1. 非財產上損害不需達「重大性」門檻，焦慮、不安等抽象感受即可構成損害。<br>2. 賠償制度僅具補償性，排除懲罰性功能。<br>3. 控制者需證明已履行適當安全措施，否則推定過失。 | 1. 強化資料主體保護機制。<br>2. 提升企業資安防護投資與訴訟防禦成本。<br>3. 確立賠償金額計算的「完全補償原則」。 |

綜合各案可見，CJEU 於 C-340/21 及 C-667/21 案中均明確採取對控制者不利



doi:10.6342/NTU202501770

的解釋方式，認為資料外洩即可能推定企業未盡適當技術與組織措施，須由其證明已採取足夠防護，否則應推定存在過失。此外，法院對於非財產損害之認定採取較寬鬆標準，認為即使無明確財產損失，若能證明受害人承受精神壓力、控制權喪失等即構成可賠償損害，如 C-300/21 與 BGH VI ZR 10/24 即肯認控制權本身之價值。

惟法院亦強調賠償範圍需符比例原則，於 C-182/22 案否定懲罰性賠償，並於 C-456/22 案中指出即便個資曾被公開，若無實質損害發生則難以構成請求基礎，凸顯法院對「損害存在」仍要求事證支持。整體而言，CJEU 實務展現出對資料控制者較為嚴格之標準，兼顧消費者保障與法律安定性，對我國實務頗具參考價值。

## 第四項 對企業責任制度的影響與制度反思

GDPR 第 82 條所確立之損害賠償責任制度，透過歐盟法院日益細緻的實務見解，已不僅是資料外洩事件之事後補償規範，更形塑為企業於資料處理全生命周期中應盡義務與法律風險防控的整體制度框架。此一發展趨勢，對企業尤其是跨境營運之數位服務提供者，帶來三方面深遠影響：

一、企業法律義務之實質化與技術化

歐盟法院不再滿足於企業提出書面政策、內部手冊或形式性合規宣稱，而是採「實質審查」與「技術標準導向」原則，要求控制者證明具體措施落實於日常營運、資訊系統設計與人員訓練中。例如，若企業未建置滲透測試、入侵偵測、雙因素驗證等已為業界常見之安全機制，將難以排除過失推定或舉證反駁。此種趨勢將合規要求實質轉化為一套技術治理責任體系，企業資訊部門與法務部門之協同整合亦成為不可或缺之基礎工程。

二、訴訟風險之高度可預測性與風險外部化效應

由於法院逐步確立可推定過失、舉證轉換、風險焦慮可賠等原則，使得資料主體在多數情境下無需證明特定行為瑕疵或實際財損，即能啟動賠償責任機制。企業如未建立完整之資料處理流程記錄、外洩應變機制與即時法律風控體系，恐面臨損害擴大後難以舉證反駁之局面。此外，由於現行歐盟各成員國仍未統一非財產損害之計算標準，企業亦需因地制宜，預先研判風險曝險程度與保險配置需求。



doi:10.6342/NTU202501770

三、制度設計上之反思與修正需求

現行以法院判例為核心所建立之「動態義務」與「擴張解釋」雖有助於保護資料主體，惟亦引發企業界對於法律安定性、成本合理性與技術可行性之疑慮。過高的安全標準門檻與不確定的損害定義，可能導致企業「過度合規」、抑制數位創新，甚至造成中小企業難以負荷的制度壓力。未來立法機關與監管機構可考慮明確區分「高風險處理活動」與「一般性資料處理」，針對不同層級義務進行比例原則之落實，並引入「合格安全標章」或「行業自律準則」作為舉證替代機制，以平衡資料保護與產業發展。

四、小結

GDPR 第 82 條損害賠償責任制度，實已躍升為歐盟資料治理體系中的核心工具，企業應不再視之為僅屬法律合規問題，而應將其內嵌於企業風險管理與數位治理架構中，強化內部監控鏈結、強化證據保存策略、制定跨部門應變機制，始能在個資外洩頻仍與司法審查深化之雙重壓力下，維持市場信譽與法律安全。



doi:10.6342/NTU202501770

# 第三章　我國個資法規定與電商平台業者之個資管理義務

## 第一節　個資法之立法背景與沿革

### 第一項 個資法之歷史背景

1995 年 8 月 11 日，臺灣制定了「電腦處理個人資料保護法」（簡稱「電資法」），旨在因應政府機關與企業大量使用電腦處理個人資料的趨勢，並參考經濟合作暨發展組織（OECD）的個人資料保護原則，保障個人資料的安全。[57]

### 第二項 個資法歷次修法沿革

一、2010 年修正

隨著資訊科技的進步，原有的電資法已無法全面涵蓋非電子化的個人資料處理活動。為此，立法院於 2010 年 5 月 26 日通過修正案，將法律名稱更改為個人資料保護法，擴大適用範圍至所有形式的個人資料處理，並取消對特定行業的限制。

二、2012 年施行

雖然 2010 年完成修法，但因部分條文（如第 6 條關於特種個人資料的蒐集、處理與利用）引發爭議，導致法案遲至 2012 年 10 月 1 日才正式施行。[58]

三、2015 年修正

為解決 2010 年修法後的實務問題，立法院於 2015 年 12 月 30 日再次修正個資法，明確規定特種個人資料的蒐集、處理與利用條件，並調整當事人同意的方式，

---

[57] 李震山（2004），〈「電腦處理個人資料保護法」之回顧與前瞻文獻引用〉，《中正大學法學集刊》，14 期，頁 48。

[58] 財團法人資訊工業策進會科技法律研究所網站，https://stli.iii.org.tw/article-detail.aspx?no=0&tp=3&i=158&d=6085（最後瀏覽日：2025/05/11）。



doi:10.6342/NTU202501770

放寬對新法施行前間接蒐集個資之告知期間等。[59]

四、2023 年修正

因應個資外洩事件頻傳，立法院於 2023 年 5 月 16 日通過修正案，強化對非公務機關違反安全維護義務的罰則，提高罰鍰上限，並規定情節重大者可處以更高額度的罰鍰。此外，明定未來將設立「個人資料保護委員會」作為專責主管機關，以統籌個資保護事務。[60]

(一) 設立個人資料保護委員會：為了建立獨立的監督機制，本次修法增訂第 1 條之 1，明定設立「個人資料保護委員會」(以下簡稱「個資會」) 作為個資法的主管機關，且其性質為獨立機關。個資會負責統籌全國個人資料保護事務，確保公務機關與非公務機關均遵守個資法的相關規定。

(二) 提高對非公務機關的罰鍰：針對非公務機關未履行個資保護義務的情況，修正案對第 48 條進行了調整，旨在促使企業投入更多資源於個資保護，減少外洩事件的發生。主要包括：

1. 直接處罰並命令改正：對於未善盡安全維護義務導致個資外洩的非公務機關，主管機關可直接處以 2 萬元以上、200 萬元以下的罰鍰，並命其限期改正。
2. 情節重大者加重處罰：若情節重大，罰鍰提高至 15 萬元以上、1,500 萬元以下。屆期未改正者按次處罰：若在限期內未完成改正，將按次處以 15 萬元以上、1,500 萬元以下的罰鍰。

五、個人資料保護委員會籌備處公告修正草案 [61]

我國個資法自 2010 年全面修正後，歷經 2015 年部分修法，惟在制度設計上

---

[59] 法源法律網（2015），〈立法院三讀通過修正「個人資料保護法」〉，https://www.lawbank.com.tw/news/NewsContent.aspx?NID=132849.00 （最後瀏覽日：2025/05/11）。

[60] 國家發展委員會（2023），〈立法院三讀通過個資法修正案將強化企業個資外洩罰責並盡速設置個資保護委員會籌備處〉，https://www.ndc.gov.tw/nc_27_36901（最後瀏覽日：2025/05/11）。

[61] 法源法律網（2025），〈個人資料保護委員會籌備處公告「個人資料保護法」部分條文修正草案〉，https://www.lawbank.com.tw/news/NewsContent.aspx?NID=206582.00 （最後瀏覽日：



doi:10.6342/NTU202501770

仍存若干缺漏。特別是公務機關的監督制度，一直處於缺乏獨立監理機構的狀態，引發外界對於個人資料保障實效之疑慮。為回應憲法法庭於 111 年憲判字第 13 號判決所揭示之違憲問題，個人資料保護委員會籌備處已於 2025 年 1 月 10 日公告修正草案，擬透過重大制度性變革，確立獨立監督機制並強化實務執行力，邁向與歐盟 GDPR 相當之現代個資治理體系。

(一) 設立「個人資料保護委員會」為獨立機關：最關鍵的修正為正式明文設置「個人資料保護委員會」（簡稱「個資會」），作為中央專責主管機關，具有獨立行使職權的地位。該設計回應憲法法庭要求建立具獨立性之監督機構，以符合憲法第 22 條所保障之資訊隱私權保障機制。個資會除對非公務機關具備傳統之執法與行政裁處職能外，亦將首度對「公務機關」行使監督職權，填補長年監理真空。其權限將包括：查核、調查、命令改正、公布違法事實、處分等完整行政監督工具，並可跨部會協調，建構統一、一元的個資治理架構。

(二) 強化個資事故應變與通報義務：草案新增第 12 條之一及第 12 條之二，要求機關在發生個資遭不法洩漏、滅失或竄改等情形時，應立即採取應變措施，並保留相關紀錄。特定條件下，應主動向個資會通報，並通知當事人。通知內容須明確揭示事故原因、被影響之資料類型、可能影響、以及應變處置與防範建議。此舉一方面提升資訊透明度，讓當事人可及時採取防範詐騙、身份盜用等風險對策；另一方面亦將促使機關強化資安防護機制，主動揭露責任，達成預防勝於處罰之政策導向。

(三) 明訂「個資保護長制度」落實內部管理責任：配合組織責任制原則，草案要求各公務機關應設置「個人資料保護長」，負責統籌內部制度建置、教育訓練、風險評估及自我檢核等事務。非公務機關部分，亦預期未來透過授權命令加以擴及。此設計與 GDPR 第 37 條對「資料保護官」（DPO）之制度有雷同性，標誌我國個資保護法治發展已逐步接軌國際，兼顧法遵與風險治理之實務需求。

---

2025/05/11）。



doi:10.6342/NTU202501770

(四) 明確化主管機關監督及處分權限：本次修法釐清主管機關得為監督之方式，包括要求限期改正、命令停止違法行為、公布違規名單等，並授權訂定行政檢查作業辦法，以利制度落實。此舉補強過往行政實務執行力不足之問題，強化震懾效果，也可作為未來風險評等或資安認證參考依據。

(五) 規劃過渡期與分階段移轉監理權限：由於目前非公務機關之主管機關分散（如金管會、教育部、衛福部等），草案規劃於個資會成立初期，先就無特定目的事業主管機關之業者優先納入統一監理；原有主管機關者得在兩年內分階段移轉至個資會，兼顧制度過渡穩定與未來一元化監理理想。

對於企業而言，修法後的罰則大幅提高，意味著需要投入更多資源加強個資保護措施，包括設置專責人員、定期進行風險評估、完善內部管理制度等。同時，強化的通報機制也要求企業在發生個資事故時，能迅速反應並採取補救措施，以減少對當事人的影響。

## 第二節　個資法規範電商業者之個資管理義務

### 第一項 電商業者適用之法律範圍與基本原則

一、合法性原則

電商業者蒐集個人資料時，須依據個資法第 5 條[62]之規定，必須具備合法正當的蒐集管道，禁止使用不正當手段取得資料，例如詐欺、脅迫或未經同意即進行個資的收集與利用。此外，若需超出原定目的使用個人資料，須事先取得當事人的明確同意，以確保資料使用的合法性。

二、目的特定原則

依據個資法第 3 條[63]與第 7 條[64]之規定，電商業者應於蒐集個資時明確告知

[62] 個人資料保護法第 5 條。

[63] 個人資料保護法第 3 條。

[64] 個人資料保護法第 7 條。



doi:10.6342/NTU202501770

資料蒐集之特定目的，並僅得於當事人同意的範圍內進行利用。任何超出特定目的的使用，均需重新取得當事人同意，例如原先蒐集用於交易的個資不得未經同意即用於其他行銷目的。

三、目的必要性原則

根據個資法第 10 條之規定，電商業者應僅限蒐集提供其服務或業務所必要之最小範圍內的個人資料。例如，在購物過程中，若非交易必要，不得強制消費者提供敏感性資料如出生年月日、收入狀況等資訊。

四、資料正確性原則

個資法第 11 條[65]要求電商業者須確保所蒐集之個人資料之正確性，並提供當事人隨時更正、補充的權利。電商業者可透過系統建置提供消費者查詢、更正與更新其資料的管道，並應主動檢視並更新不正確或過時的資料，以確保資料正確與完整。

五、安全保障原則

依據個資法第 12 條[66]規定，電商業者須對其蒐集的個人資料採取合理的技術與管理措施，例如加密儲存、防火牆部署、身份認證措施、定期安全稽核等，以防止資料未經授權之存取、洩漏、竄改與損毀。

六、透明告知與當事人權利

個資法第 8 條[67]及第 9 條[68]明確要求電商業者在蒐集個人資料時應清楚告知當事人蒐集的目的、用途、資料保存期間、第三方分享情形，並提供當事人查詢、更正、刪除資料及拒絕行銷等權利之行使機制。

---

[65] 個人資料保護法第 11 條。

[66] 個人資料保護法第 12 條。

[67] 個人資料保護法第 8 條。

[68] 個人資料保護法第 9 條。



doi:10.6342/NTU202501770

### 第二項 個人資料之蒐集及告知義務

電商業者在個人資料蒐集階段，應清楚符合個資法第 8 條[69]及第 9 條[70]的規定，於收集資料時即明確告知消費者相關資訊，包括資料的具體用途、處理方式及保存期限。常見的電商資料蒐集範圍包括姓名、聯絡資訊、電子郵件、支付資訊及網站使用行為紀錄。業者亦應避免蒐集與交易無關或不必要之個資，以減少法令遵循之風險。

### 第三項 個人資料的處理與利用規範

電商業者在處理與利用個資時，須建立嚴謹內控機制，依照數位經濟相關產業個人資料檔案安全維護管理辦法第 9 條[71]的規定，確保處理活動符合法定情形及特定目的，並明確界定個資之內部存取權限。若涉及國際資料傳輸，應遵守該管理辦法第 10 條[72]規範，確認境外資料接收方有足夠的資料安全保護措施，並事先告知消費者。

### 第四項 資料安全管理與應變措施

數位經濟相關產業個人資料檔案安全維護管理辦法第 11 條[73]進一步強化電商業者之資料安全管理義務，要求業者透過加密、防火牆、入侵偵測及資安監控機制，防範外部攻擊與內部未經授權存取。此外，業者亦須訂定嚴謹的事故應變機制，發生事故時於 72 小時內通報主管機關，並即時通知當事人，以降低資料事故所造成之潛在損害。

---

[69] 個人資料保護法第 8 條。

[70] 個人資料保護法第 9 條。

[71] 數位經濟相關產業個人資料檔案安全維護管理辦法第 9 條。

[72] 數位經濟相關產業個人資料檔案安全維護管理辦法第 10 條。

[73] 數位經濟相關產業個人資料檔案安全維護管理辦法第 11 條。



doi:10.6342/NTU202501770

### 第五項 委外處理與監督管理

電商業者若委託第三方進行個資處理，依據數位經濟相關產業個人資料檔案安全維護管理辦法第 19 條[74]規定，須明訂委外處理契約，確保第三方符合相同的資料安全保護標準，並定期進行檢視與稽核，以確保委外廠商落實保護措施，避免因委外過程疏忽而造成個資外洩。

電商業者在數位經濟時代承擔重要的個資管理義務，必須積極履行法律規範，落實各項個人資料保護措施。透過嚴格執行個資蒐集、處理及利用之合法性、透明性、必要性與安全性原則，業者可降低潛在的法律風險，提升消費者信任度，進而促進電商產業的健康且永續的發展。

## 第三節　企業如何符合個資法第 27 條適當安全維護措施之標準

隨著數位經濟與網際網路應用的蓬勃發展，企業、政府及其他組織在進行資料蒐集、處理與利用時，面臨前所未有的資訊安全挑戰。特別是在電子商務、金融服務、醫療保健等高風險產業，個人資料的保護成為社會關注焦點。為因應外部駭客攻擊、內部管理疏失以及其他可能導致個資外洩的風險，立法機關制定了個資法及其施行細則，其中第 27 條規定了業者必須建立「安全措施與維護計畫」，而施行細則第 12 條則進一步明訂「適當的安全措施」的具體內容。這兩項規定既從戰略層面要求業者建立整體防護藍圖，也從操作層面提出了技術、行政與物理防護之具體要求。本文旨在就上述法條內容進行詳細介紹，探討各項規範之立法背景、具體要求與實務落實情形，並分析業者在建置資安防護體系時所應採取的對應措施及未來發展方向數位經濟相關產業個人資料檔案安全維護管理辦法。

[74] 數位經濟相關產業個人資料檔案安全維護管理辦法第 19 條。



doi:10.6342/NTU202501770

## 第一項 個資法第 27 條：安全措施與維護計畫

### 一、立法背景與目的

個資法第 27 條的制定，源自於對個人資料在網路環境中易遭竊取、竄改或毀損之現實風險考量。隨著企業越來越依賴數位資料進行經營管理，單一的事後處理機制已難以應對日益複雜的資安挑戰。因此，立法者主張必須從源頭出發，要求業者在資料全生命週期中，均應納入系統化、制度化的安全防護措施。此舉不僅有助於防範事故發生，同時也為發生意外時提供明確的責任認定依據。透過訂定安全維護計畫，業者應先行進行風險評估，針對蒐集、處理、儲存與傳輸等各環節訂定防護標準與應變措施，以達到預防、偵測與因應之目的。

### 二、規範內容概述

根據個資法第 27 條[75]，業者須在法定期限內（多數規定為施行日起三個月內）完成安全維護計畫之訂定，並應定期檢討、更新與修正。該計畫主要涵蓋下列幾個重點：

(一) 內部資料保護政策

1. 制定明確的資料保護政策，規範資料蒐集、處理、儲存、傳輸及銷毀的全過程。
2. 明確劃分各部門與員工在資安管理中的職責，確保所有從業人員均了解並遵守相關規定。

(二) 風險評估與辨識

1. 根據業務性質與處理資料的敏感程度，定期進行風險評估。
2. 評估結果應作為安全維護計畫調整與防護措施配置的重要依據，確保資安風險能夠及時識別並加以控管。

(三) 技術與管理措施

1. 根據風險評估結果，針對不同風險層級採取相應的技術防護與管理控制措施。

---

[75] 個資法第 27 條。



doi:10.6342/NTU202501770

2. 技術措施包括加密、防火牆、入侵偵測系統、資料備份及系統漏洞掃描等；管理措施則涵蓋內部權限控管、定期稽核、資安教育與員工培訓等。

(四) 事故應變機制

1. 建立完善的應變計畫，包括事故發生後的調查、損害降減、通報流程及後續改善措施。

2. 制定清晰的事故通報標準，並規定受影響者通知及主管機關通報的時限與方式。

(五) 持續改善與稽核

1. 建立內部稽核機制，定期檢查安全維護計畫之執行情形。

2. 保存各項措施實施的證據與紀錄，以便日後追溯與監督，並依照技術發展及業務調整進行動態修正數位經濟相關產業個人資料檔案安全維護管理辦法。

三、企業具體對應措施

企業在落實個資法第 27 條規定時，通常會依據以下步驟進行：

(一) 初期風險評估與規劃

1. 透過專業顧問或內部資訊安全團隊，對現有資訊系統進行全面的風險評估，識別潛在的漏洞與弱點。

2. 根據評估結果，制定安全維護計畫，列明各項防護措施、執行標準及資源分配情形。

(二) 內部管理制度建構

1. 建立資料保護管理政策文件，明訂各級人員的權責分工，並對涉及個資處理的人員訂立保密協議。

2. 設定資料存取權限，並利用技術工具監控員工的資料存取行為，以防範內部濫用。

(三) 技術防護措施落實

1. 對敏感資料採取加密技術，確保無論在傳輸或存儲過程中，均不易被未經授權



doi:10.6342/NTU202501770

者竊取或讀取。

2. 配置防火牆、入侵偵測系統及防毒軟體，並定期更新軟硬體設備，確保防護系統能應對最新型態的網路攻擊。

(四) 應變機制與演練

1. 制定事故應變計畫，規劃各類資安事件發生時的緊急處理流程。

2. 定期舉行資安演練，模擬外洩或攻擊事件，檢驗應變計畫的有效性，並根據演練結果持續修正完善。

(五) 紀錄與稽核

1. 將安全維護計畫的執行情形、檢查結果與改善措施以書面形式記錄並保存，滿足監管要求。

2. 定期進行內部稽核，必要時邀請第三方機構進行獨立檢查，確保資安措施不斷更新且符合現行法規要求。

## 第二項 個資法施行細則第 12 條：適當的安全措施

### 一、立法背景與目的

個資法施行細則第 12 條[76]的核心在於對個資法第 27 條中「安全措施」的概念予以進一步細化與具體化，使業者在實際操作時能依據明確標準來落實防護措施。由於技術環境不斷演進，單靠抽象的規範已無法滿足資訊安全需求，因此施行細則從技術、行政與物理三大層面，分別列出應採取的安全措施，旨在促使業者根據實際情況及最新技術水準，制定並實施一系列具體的防護作法。

### 二、規範內容概述

(一) 技術性安全措施

1. 資料加密：對於需保護之敏感資料，無論在資料蒐集、儲存或傳輸過程中，都

[76] 個資法施行細則第 12 條。



doi:10.6342/NTU202501770

應採用國際通用的加密演算法，防止資料遭竊或非法竄改。

2. 防火牆與入侵偵測系統：建置防火牆、電子郵件過濾系統以及入侵偵測設備，有效阻擋外部不法存取與駭客攻擊，並定期更新規則以應對新型態威脅。

3. 備份與異常監控：建立定期資料備份機制，確保一旦資料因系統故障或攻擊而受損，能迅速還原；同時透過異常監控系統及時偵測非正常存取行為，並觸發警報。

4. 安全傳輸機制：針對網路傳輸，採用安全通訊協定（如 SSL/TLS），確保資料在傳送過程中不被竊聽或竄改。

(二) 行政性安全措施

1. 內部管理規範制定：業者需編製個人資料保護管理規範，明訂資料存取權限、資料處理流程、資料保留期限及銷毀標準，並對外公告以強化內部監督。

2. 人員管理與培訓：

(1) 與涉及個資處理之員工簽訂保密協議，約定保密義務與違約責任。

(2) 定期舉辦資安法令、內部規範及事故應變培訓，提升員工對個資保護重要性的認知。

3. 權限控管與審核：透過資訊系統對各層級人員設定不同的資料存取權限，並定期進行權限審查，避免因人員調動或系統漏洞導致的資料濫用或外洩。

4. 物理性安全措施

(1) 設備與設施保護：對存放個人資料的實體設備（如伺服器、硬碟）採取防火、防盜、防水措施，並在存放區域設置出入管制與監視系統。

(2) 環境控制：針對資料儲存環境進行溫度、濕度等環境監控，確保設備處於安全穩定狀態；同時設置緊急停電、火災警報等裝置，降低外部意外因素對資料安全的影響。

三、具體對應措施與實務應用

依據施行細則第 12 條規定，業者在具體落實「適當的安全措施」時，可從下



doi:10.6342/NTU202501770

列方面著手：

(一) 技術層面的具體作法

1. 針對敏感資料，採用高強度加密軟體（如 AES-256）進行資料加密，並確保金鑰管理制度完善。
2. 建置並定期更新防火牆、入侵偵測系統與防毒軟體，並利用即時監控工具追蹤網路異常活動。
3. 設置自動備份系統，並將備份資料存放在不同地理位置，以應對災害或系統故障；同時，定期進行備份復原測試，確保備份資料的可用性。
4. 對於資料傳輸，採用加密通道（如 VPN、SSL/TLS），並設置防止中間人攻擊的安全機制。

(二) 行政層面的具體作法：

1. 編製並公開企業內部個人資料保護政策，確保所有員工皆了解政策內容與違規後果。
2. 相關人員簽訂保密協議，並設置專門的資安管理團隊或指定資安負責人，定期檢查及推動安全措施的落實。
3. 期舉辦內部資安培訓與演練，並邀請外部專家進行資安講座，提升全員的安全意識。
4. 設立內部稽核機制，定期審查資料存取權限、操作記錄以及系統異常報告，並形成書面稽核報告，便於主管機關查核。

(三) 物理層面的具體作法

1. 對於存放個人資料的伺服器機房，必須採取嚴格的實體進出管制措施，如電子門禁、指紋辨識或門禁卡管理，並設置監視器全天候監控。
2. 設置適當的環境監控系統，包括溫濕度監控、煙霧偵測、火災警報系統等，並定期檢查相關設備的運作狀態。對重要設備進行定期維護與檢修，確保硬體狀況穩定，避免因設備故障導致資料損毀或外洩。



doi:10.6342/NTU202501770

# 第四章　我國個人資料外洩民事損害賠償責任之實務判決分析

隨著資訊科技與網路經濟的迅速發展，企業於日常經營中大量蒐集、處理及利用個人資料已成為不可或缺的作業模式。然而，資料庫安全漏洞與管理疏失使得個人資料外洩事件頻傳，進而引發民事損害賠償訴訟。臺灣法院在審理此類案件時，除了依據民法關於侵權行為的基本規定外，更須結合個資法的特殊規範與推定過失責任原則，對企業是否盡到安全防護義務、資料外洩與消費者損害之間是否構成相當因果關係、以及雙方舉證責任如何分配進行細緻審查。

本章將對臺灣法院近年來涉及個資外洩案件之判決進行系統性分析，探討不同判決結果間的差異性與原因，並從侵權行為的成立要件、過失認定、舉證責任分配、因果關係認定、企業安全義務、通知補救措施及損害賠償範圍等多個角度，剖析判決中的爭議點與司法考量，以期呈現臺灣法院在處理此類案件時所採取的多元裁判模式，並為未來法律實務與立法完善提供參考。

## 第一節　我國法院實務判決分析

### 第一項 橘熊科技股份有限公司（OB 嚴選）個資外洩案

裁判字號：臺灣士林地方法院 107 年度湖小字第 401 號民事判決

一、案件事實

(一) 原告起訴主張：原告曾於被告橘熊科技股份有限公司（下稱橘熊公司）經營之「OB 嚴選」網站消費並留下個人資料。民國（下同）106 年 10 月 21 日，原告接獲自稱為該公司會計人員之電話，對方稱因公司內部電腦系統出錯造成多筆購買資料需轉由銀行協助處理，並能準確說出原告之購物日期、商品內容及手機號碼、住址等資訊。原告一度信以為真，經家人提醒方察覺異常並掛斷電話。事後經 165 反詐騙專線與信用卡公司確認，該通電話為詐騙集團所為。原告主張，其個資應係自被告橘熊公司處洩漏，否則第三人無從得知具體消費資訊。被告橘熊公司未依個資法善盡安全維護義務，致原告個資遭不法取得並進行精準詐騙，令原告受有非財產上損害，爰依個資法第 29 條請求被告橘熊



doi:10.6342/NTU202501770

公司賠償新臺幣（下同）2 萬元之精神慰撫金。

(二) 被告橘熊公司抗辯

1. 原告接獲之詐騙電話內容屬常見詐騙話術，原告本應有所警覺。

2. 被告橘熊公司一向重視資安管理，已依個資法建置個資安全維護計畫，網站並採用 DoS/DDoS 攻擊防護系統，亦定期委託第三方資安公司進行弱點掃描，迄今未發現任何內部資料外洩之跡象。

3. 原告個資可能因自身於不安全網路環境中點擊惡意連結、未定期更換密碼或裝置遭植入木馬程式而洩露。此外，物流業者、超商或大樓管理人等亦可能掌握原告之個資與消費訊息，難以推定資料即來自被告橘熊公司。

4. 被告橘熊公司已盡資安維護義務，與原告所稱損害間不具因果關係，亦無故意或過失。

二、法院判決理由[77]

(一) 某詐騙集團取得系爭消費資訊是否因被告橘熊公司未善盡保護責任所洩漏：

1. 法院採用「常態事實」與「變態事實」之區分，作為舉證責任分配的依據。依據此理論，若某一事實依照社會經驗與一般常態應由特定行為人負責，則主張此一「常態」事實者可免舉證；反之，欲主張反常可能（即「變態」事實）者，則須負較高程度之舉證責任。法院指出，被告橘熊公司經營網路購物平台，資本額達數億元，並於其網站、資料庫等處理並儲存大量客戶個資與交易資訊，屬於一般商業常態。而相對而言，消費者如原告僅為個人使用者，其手機或個人電腦保有部分個資，卻發生被詐騙集團準確掌握「購物日期、商品名稱、聯絡方式」等細節，顯然不符合資訊流通常態。在此情形下，被告橘熊公司主張該資訊可能源自其他第三方（例如物流業者、便利商店或原告誤用裝置），即屬「變態事實」，應自負高度舉證責任。

2. 法院進一步指出，原告已提出包含信用卡帳單、通聯紀錄以及新聞報導（指出

[77] 臺灣士林地方法院 107 年度湖小字第 401 號民事判決。



doi:10.6342/NTU202501770

OB 嚴選平台有大量個資外洩案件，並列為警方統計之前五名）等證據，加上被告橘熊公司亦無法提出可排除其責之佐證，即便被告橘熊公司否認與本案個資外洩有關，亦辯稱其他可能來源非全然無根，但在現有證據偏在企業、資訊落差懸殊的背景下，法院採取推定方式認定，該筆個資應係由被告橘熊公司內部或其掌控系統中洩出，為較合理之解釋。法院據此確立，若無法提出反證說明已妥善保存顧客個資，則應推定企業未盡保護責任。

(二) 被告橘熊公司是否已依個資法第 27 條採取適當安全措施，無過失？

1. 法院透過實質審查的方式檢視其主張之資安防護機制，並據以判斷是否已盡法律所要求之注意義務。雖然被告橘熊公司聲稱已建置多項資安設備與制度，包括如 Arbor Networks 阻斷式攻擊防護、FortiGate 防火牆、Imperva 應用程式防火牆（WAF）、定期網站弱點掃描、對內部人員之嚴格控管機制等，表面上顯示其已有相當重視資安問題，但法院認為僅憑列舉技術項目與抽象主張，並不足以證明其實際落實資安防護義務。實務上「資安管理」並非僅止於設備安裝，而應包含其規劃、建置、執行、稽核、檢討等完整程序，特別是在發生資料外洩事件之後，更須提出足以證明曾採行有效防範措施之事後證據。

2. 法院指出，被告橘熊公司未能提出任何建置文件、內控規章或第三方稽核報告等實據，以佐證其主張資安系統早已建構並運作良好。此外，其對於人員管控制度之聲明亦未附具訓練紀錄、職責分工或違規懲處機制等內容，使得該部分主張流於空泛。法院認為，資訊安全義務並非僅存於「設備設置」之形式，而應落實至企業內部實際運作層面，否則形同空殼。加上法院亦援引媒體報導指出「OB 嚴選」網站疑有數十人個資外洩，且被告橘熊公司亦坦承曾接獲警方通知後再度檢視系統安全情形，顯示其對資料外洩風險早有掌握可能。最終，法院認為，在無其他佐證資料的情形下，被告橘熊公司難以舉證其已採取「適當」安全措施，因此應推定其未善盡個資保護義務，對於個資外洩事故存有過失。

(三) 被告橘熊公司過失與原告損害間是否具相當因果關係？

1. 在確認被告橘熊公司具過失之後，法院進一步審酌本案中原告所主張之損害是否與被告橘熊公司過失間存在「相當因果關係」。法院特別指出，因果關係的認



doi:10.6342/NTU202501770

定雖原則上應由請求損害賠償者（即原告）負舉證責任，惟民事訴訟法第 277 條但書明定，在舉證若顯不公平之情況下，法院可酌情調整證明責任與程度。法院認為，個資外洩案屬於高度專業化、技術性強、證據偏在企業一方之現代型訴訟，類似於商品責任、公害或醫療糾紛等領域，傳統舉證規則難以兼顧實質正義。法院因而援引最高法院 103 年度台上字第 1311 號判決，及 102 年度台上字第 31 號判決所採「危險領域理論」與「相當合理確定性」推定標準，認為可對企業行為所產生的風險作出合理推論與責任歸屬。

2. 法院指出，被告橘熊公司作為資料控制者，對原告交付之個資擁有管理與保護義務，其對於風險之控制能力明顯優於個別消費者。當發生個資外洩並遭不法第三人利用進行精準詐騙，若企業僅以抽象否認或主張「無直接證據證明來源」即推諉責任，將使受害者永遠無從舉證，而無法獲得法律救濟。因此，本案法院認定：在已確認被告橘熊公司有資安管理過失、且存在個資外洩客觀事實的情況下，即可推定其與原告所受非財產上損害間具備相當因果關係。倘被告橘熊公司認為不存在因果關係，則應自行提出具體反證；然本案中被告橘熊公司並無具體佐證資料可排除此推定，法院因此認為原告之請求具有法律依據，賠償請求應予准許。

3. 綜上，法院認定原告之個資外洩與被告橘熊公司未善盡法定維護義務之間，構成法律上之相當因果關係，原告依個資法第 29 條、第 28 條第 2 項請求非財產上損害賠償 2 萬元，於法有據，並衡情適當。

三、判決影響與未來發展之分析

(一) 首先，在舉證責任分配的調整方面，法院採用「常態事實／變態事實」之二分法，認為被告橘熊公司作為經營大型電商平台之企業，對於收集、儲存並處理客戶個資已成商業模式之常態，應自負說明與舉證責任。法院據此指出，若企業未能具體證明其已落實保護措施、未導致外洩，則即便原告無法直接指出外洩管道，仍可推定資訊源於企業內部流出，屬可歸責於企業之事實。此一論理與德國聯邦最高法院（BGH）2024 年判決（VI ZR 10/24）所採見解相似，該案亦認定若資料控制者未能證明其系統未出現漏洞，則應推定外洩事件與其作為具因果關係。橘熊案展現出我國法院逐步意識到「資訊不對等」所導致之



doi:10.6342/NTU202501770

證明困難，藉由舉證責任重分，降低消費者在數位平台下的弱勢地位，有助提升個資保護法的救濟實效性。

(二) 再者，於企業過失判斷與合規責任實質化方面，橘熊案判決拒絕僅以被告「列舉資安設備」即認其無過失。法院要求被告提出具體建置證明、使用紀錄、委外稽核報告等資料，以證明其資安制度不僅形式存在，亦實際落實。法院強調，僅列示資安系統名稱與設備型號，不足以證明其有效性與持續執行，更遑論達到個資法第 27 條所要求之「適當安全措施」標準。此種對企業內部控管實踐的實質審查，呼應 GDPR 第 32 條所規範的「組織與技術安全措施」需依據風險動態調整並具有效性原則，顯示我國法院已不再滿足於「符合法定文字」的紙上合規，而轉向檢驗「實務成效」的動態監督標準。未來實務或可進一步發展出「可稽核性合規責任」（accountability-by-evidence）原則，要求企業在面對個資爭議時，須提出足以說服法院之紀錄與證據，而不僅止於技術名稱或程序宣示。

(三) 此外，橘熊案判決最具突破性的部分，在於對因果關係之推定方式採寬鬆標準。法院指出，若依傳統民法上「原告需證明加害行為與損害間具直接因果關係」之原則，將造成受害人因舉證困難而無法救濟，顯失公平。參照民事訴訟法第 277 條但書，法院認為在資訊非對稱的情境下，應考慮被害人與企業間之能力落差、證據偏在與技術屏障，調整因果關係之證明負擔。法院比照我國公害與醫療訴訟實務，援引「危險領域理論」與「合理確定性推定」標準，認為企業若對資料擁有實質支配力，且管理顯有疏失，即可推定其行為與損害具相當因果關係。該推定原則與 GDPR 第 82 條實務解釋亦頗為接近，後者亦傾向將證明外洩與損害之連結義務加諸資料控制者，除非企業能證明外洩與己無關，否則應承擔賠償責任。此一因果關係推定方式，對未來跨境資料流通、雲端資料外洩或系統攻擊來源不明之案件，提供具實用性的司法標準，並可避免企業以「無法查明來源」為由推諉責任，進而強化企業之預防義務與內控動機。

(四) 從制度發展的角度來看，本案對我國未來個資法修法或行政指導方向具有重要啟示。雖然現行個資法第 29 條已明定「過失推定」原則，資料控制者如未善盡安全維護責任，於發生個資外洩時即推定其有過失，惟現行規範對於「因



doi:10.6342/NTU202501770

果推定」、重大外洩事件之「舉證責任轉移」等細節，尚有進一步明確化與制度化的空間。為避免標準分歧與適用不一，未來立法機關可考慮：參考 GDPR 規範體系，進一步明文化資料控制者於特定情形下的「證明責任」與「舉證責任轉移」機制。針對重大個資外洩事件，建立更明確的推定條款，強化受害者權益保障及促進企業自律。結合現有個資評鑑制度，建構一致性的行政與司法審查標準，提升法規適用之明確性與可預期性。推動資訊揭露制度，要求重大平台業者定期揭露資安事件處理狀況與風險因應機制，促進企業風險意識與社會監督。總結來說，雖然個資法第 29 條已有「過失推定」規定，但為因應新型態個資外洩風險與國際規範趨勢，仍有必要就「因果推定」、「舉證責任轉移」及資訊揭露等面向，進行更細緻的制度設計與修法規劃，以強化我國個資保護體系的完整性與實效性。

## 第二項 雄獅旅行社股份有限公司 107 年個資外洩案

裁判字號：臺灣士林地方法院 107 年度消字第 6 號民事判決

一、案件事實

(一) 原告起訴主張:原告財團法人中華民國消費者文教基金會依據個資法第 32 條、第 34 條，取得 25 名受害人之訴訟實施權後，以自己名義對被告被告雄獅旅行社股份有限公司（下稱雄獅旅行社）提起團體損害賠償訴訟。原告認為被告雄獅旅行社經營旅行業務，依法蒐集消費者個人資料，惟未妥善建立及維護資訊安全管理機制。106 年 5 月，被告雄獅旅行社系統遭不明人士以員工帳號入侵，致消費者個資（包括姓名、電話、住址、身分證字號等）外洩。此後，部分受害人即接獲冒用被告雄獅旅行社員工身分之詐騙電話，詐騙者掌握其消費資訊，藉詞誆稱交易錯誤需取消分期付款，引導被害人至 ATM 操作轉帳，造成具體財產損害；另有部分受害人雖未匯款，然因個資外洩而產生不安與精神壓力，主張非財產上損害。被告雄獅旅行社未盡保護個人資料之安全維護義務，構成個資法第 29 條第 1 項、第 2 項、第 28 條第 2 項所稱違法處理個資行為；同時，作為提供服務之企業，被告雄獅旅行社亦違反消費者保護法第 7 條第 3 項對消費者安全應負之責任，並涉民法第 227 條、第 227 條之 1 所定契約附隨義務，以及第 184 條第 1 項前段與第 2 項之侵權行為責任。請求法



doi:10.6342/NTU202501770

院判命被告雄獅旅行社給付各受害人合計損害金額 363 萬 9,592 元及利息。

(二) 被告雄獅旅行社抗辯

1. 資安事件無過失：被告雄獅旅行社公司作業系統係遭受駭客惡意入侵，屬突發非法攻擊事件，並非因違反個資法或有可歸責之過失所致。事故發生後，已即時發佈通知、公告聲明，提醒消費者防範詐騙，足認其已盡善良管理人之注意義務。

2. 原告未證明資料來源與損害存在：原告並未舉證證明附表 1-A-2、1-B 所列人員確有遭受詐騙，亦未證明詐騙者所使用之個人資料確係來自被告雄獅旅行社遭駭系統所洩漏，亦未具體證明其財產上或非財產上實際損害。縱使受害人確有損失，該等損害亦係由不法第三人詐欺行為所致，與被告無相當因果關係，且本件並無舉證責任轉換或減輕之適用情形。

3. 原告亦有過失：即使認有損害發生，如附表 1-A-2 所列人員於接獲可疑電話後未加查證，即依指示操作匯款，應對自身財產損失與有過失，不得全由被告雄獅旅行社負責。

4. 契約關係已消滅，無從主張債務不履行：被告並指出，其與相關人員間契約關係已終了，不存在後契約義務或附隨義務之問題。且個人資料保護為法定義務，非屬契約義務，雙方間亦非消費關係，自不得援引消費者保護法或民法債務不履行之規定為請求依據。

二、法院判決理由[78]

(一) 原告不得依個資法第 29 條第 1、2 項、第 28 條第 2 項規定請求被告雄獅旅行社負損害賠償責任。

1. 原告應舉證證明被告雄獅旅行社違反個資法安全維護義務：法院指出，原告依個資法第 29 條主張損害賠償，須先證明被告雄獅旅行社有違反第 27 條安全維護義務之具體事實。雖第 29 條第 1 項設有過失推定，但仍須由原告舉證業者

[78] 臺灣士林地方法院 107 年度消字第 6 號民事判決。



doi:10.6342/NTU202501770

未建立或執行符合法定標準的安全維護措施，例如未依主管機關公告採取必要技術與管理機制，否則無法成立請求。

2. 新聞報導與行政資料不足以證明資安疏失：原告援引新聞稿、警方通報與觀光局處分等資料，主張被告雄獅旅行社有資安瑕疵。法院認為，該等資料僅說明外洩經過與公司因應作法，未具體指出被告雄獅旅行社承認違規或資安管理不當。警方與媒體資訊多為被告自行說明之內容，非經調查認定；另觀光局裁罰係屬其他個資案，與本案無關，亦無法作為舉證依據。

3. 被告雄獅旅行社已提出完備資安制度並實際執行，符合法定標準：法院認為被告雄獅旅行社已建立個人資料檔案安全維護計畫，涵蓋人員權限控管、資料加密、內部稽核、資安教育及密碼管理等措施，內容與交通部觀光局公告之旅行業資安標準範本一致。且被告雄獅旅行社亦提出具體執行資料，包括稽核紀錄與訓練紀錄，足以證明其制度落實，無違反安全維護義務。

4. 資料外洩係駭客非法入侵所致，非被告雄獅旅行社可歸責之原因：雙方均不爭執個資外洩原因為駭客侵入被告系統。法院指出，縱使業者採取安全技術措施，仍可能面對外部攻擊，無法以資料外洩的發生，即推論為管理疏失或違反法律。若僅因洩漏結果就認定業者有過失，將導致企業處於無限擴張之風險責任，於法不合。

5. 與他案裁判事實基礎不同，無法比附適用：原告引用臺灣士林地方法院 107 年度湖簡字第 110 號民事判決為例，主張本案應類推適用該案見解。但彼案中被告雄獅旅行社未提出任何資安制度與落實證據，故被認定違法；本案中則不同，被告雄獅旅行社已具備完整資安機制並提出執行佐證，兩案事實基礎差異明顯，無從比附。

6. 綜上，原告未能具體證明被告違反個資法第 27 條安全維護義務，亦無證據顯示被告於資安管理上有可歸責之過失。既無違法，亦無過失，法院認定原告依第 29 條提起之損害賠償請求無理由，應予駁回。

(二) 原告不得依消費者保護法第 7 條第 3 項主張損害賠償責任：

1. 原告另主張，被告雄獅旅行社提供之旅遊服務包含個資保管義務，其若未善盡



doi:10.6342/NTU202501770

義務而導致個資外洩，即屬消保法第 7 條所稱提供「不具合理安全性之服務」，應負無過失損害賠償責任。

2. 法院首先指出，旅行業者提供票券代購、訂房等服務，因其性質必須蒐集並使用消費者之個人資料，因此消費者對資料安全存在合理期待，被告對該資料之安全管理，自屬其提供服務之一環。然依消保法第 7 條第 3 項與第 7 條之 1 規定，雖企業經營者需證明其商品或服務符合當時科技或專業水準可合理期待之安全性，但損害事實與該服務間仍須具備「相當因果關係」，此部分之舉證責任仍由消費者承擔。原告所提出之新聞稿內容僅證明個資外洩事件之發生及被告雄獅旅行社之通報措施，尚難據以證明該事件與原告所主張之財產損害具因果關係。且即使存在資料外洩事實，亦不必然導致財產損害，尤其本件尚有第三人之故意詐騙介入行為，已中斷資料外洩與財產損害之因果關係鏈條。加之，被告雄獅旅行社於事件發生後即時通知消費者、報警、召開記者會並加強防護措施，已善盡警示與補救義務。

3. 法院最後指出，消保法第 7 條雖為無過失責任，但對「因果關係」部分並無舉證責任轉換之規定，且本件並無證據偏在或顯失公平情形，不得援引民事訴訟法第 277 條但書轉換因果關係之舉證責任。綜上，原告依消保法所為之主張，亦難成立。

(三) 原告不得依民法第 227 條第 1 項、第 227 條之 1 主張不完全給付責任

1. 法院審酌原告依契約不完全給付為基礎之主張，認為保管消費者個資雖非主給付義務，然為實現旅遊服務給付目的所必要，確實屬於契約之附隨義務，從而可構成債務人（即被告）於履行契約過程中應負之保護義務。

2. 惟法院亦重申，原告主張不完全給付責任，仍須舉證損害發生與契約義務未履行間有相當因果關係。本件中，資料外洩係第三人惡意入侵所致，非可歸責於被告雄獅旅行社之事由；且原告未能證明其財損與外洩資料間具相當因果關係。故即使被告雄獅旅行社有附隨義務，亦難認其負擔不完全給付之損害賠償責任。

(四) 原告不得依民法第 184 條主張侵權行為損害賠償



doi:10.6342/NTU202501770

1. 關於侵權行為，法院指出民法第 184 條第 1 項與第 2 項規定，損害賠償之成立需具備故意或過失、不法行為及與損害結果間具相當因果關係三大要件。原告應對上述三項負舉證責任。

2. 本案中，被告雄獅旅行社已提出其有依據個資法採行適當之保護措施，且個資外洩原因係駭客入侵，被告雄獅旅行社無從預見與避免，並未具備過失。進一步而言，即使原告遭受詐騙，其損害亦非直接因被告之行為所致，而係因第三人之獨立不法犯罪行為，與被告雄獅旅行社之作為不具相當因果關係。

3. 法院亦駁斥原告所主張之違反個資法即應構成侵權行為之論點，理由在於原告未能證明被告雄獅旅行社違反任何保護法規之行為。故此一侵權行為請求，無事實依據與法律依據。

(五) 綜合而論，法院針對原告所援引之各項法律依據，包括個資法之損害賠償請求條款、消費者保護法第七條關於企業經營者無過失責任之規定、民法第 227 條及第 227 條之 1 關於契約不完全給付之責任，以及第 184 條有關侵權行為之一般與特別構成要件，逐一進行實體審查後，均認定原告之請求未能舉證證明其主張所依賴之法律構成要件，包括被告是否存有違法行為、可歸責性（即故意或過失）以及該行為與原告主張之財產損害間是否存在相當因果關係。尤其在因果關係之判斷上，法院明確指出資料外洩係由第三人駭客行為所致，屬難以預見並防止之惡意不法介入，已中斷資料外洩與損害結果之因果關係鏈條，從而排除被告雄獅旅行社就原告之損害承擔法律責任之可能性。基於上述綜合判斷，法院最終駁回原告之全部請求，並認為既然本訴欠缺實體理由。

三、判決影響與未來發展之分析

本案為國內個資外洩與詐騙損害連結的經典訴訟案例，法院最終認定原告消基會主張無證據證實被告雄獅旅行社違反個資法，也否定消費者受詐與被告雄獅旅行社個資外洩之間具備「相當因果關係」，因而駁回原告請求。

(一) 肯認個資保護義務屬企業法定義務，但仍須具體舉證違反情節：本案判決再次確認，企業對所蒐集之個人資料負有個資法第 27 條所定安全維護義務，且該義務非僅形式存在，應落實於內部制度設計、技術防護措施及人員管理等層面。然而，法院亦明確指出，原告即便可依第 29 條主張損害賠償，仍須負責



doi:10.6342/NTU202501770

舉證業者確有違反法定義務之行為。換言之，過失推定雖存在，惟非無條件適用，仍須先建立違法事實作為前提。此舉有效防止原告僅憑資料外洩結果即主張業者違法，有助實務建立責任認定的合理門檻。

(二) 強調「外洩事實」與「資安違失」不可畫上等號，避免結果歸責擴張：判決對於駭客入侵所造成的外洩事件，採取較為嚴格的因果評價標準。法院指出，資訊系統再怎麼防護亦難保絕對安全，駭客攻擊屬外力介入，若企業已建立並執行安全機制，僅憑資料外洩結果，尚不足以推論資安違失或管理過失。此種區隔「結果」與「行為」的判斷，對於日後企業遭遇類似事件時能否免責，提供了更為具體可行的審查框架，有助避免實務落入事後結果歸責的窠臼。

(三) 明確資安制度之「積極舉證」為企業抗辯關鍵：本案中，法院對於被告所提出的個資保護計畫給予高度肯認，指出其內容包括權限控管、密碼管理、教育訓練、內部稽核等，且實際有執行紀錄與證據支持。這顯示，法院在審酌企業是否盡到安全維護義務時，不僅看形式制度是否存在，更重視執行成效與證據呈現。此判斷標準鼓勵企業平時即應備妥資安稽核報告、操作紀錄、訓練紀錄等，以便於發生糾紛時作為抗辯依據，強化企業合規管理意識。

(四) 因果關係之認定仍採嚴格標準，消費者須自證詐騙損害與外洩間連結：在因果關係評價部分，法院認為雖個資確已外洩，然消費者遭詐騙之結果係由第三人詐術所致，且難以證明詐騙行為與被告所洩資料間具「相當因果關係」。法院未採取推定關聯或減輕舉證標準，而要求原告具體證明詐騙所使用之資料與其留存於被告處之個資一致，且排除其他可能來源。此一標準與風險社會中強調「資料密集業者應負資訊風險責任」的思潮不同，仍較偏向傳統過失責任下的「結果證明論」，對消費者構成較高舉證門檻。

(五) 對類案裁判採取區辨立場，強調證據基礎差異的重要性：法院在面對原告主張類推引用其他判決時，明確指出彼案業者未提出資安防護資料，而本案中被告具備完整制度與執行證據，故兩案事實不同，不應類推適用。此舉展現法院在處理類型化案件時，重視個案證據差異，避免以往裁判見解一體適用，進而維持裁判之個別化與妥當性。

(六) 綜合而言，本案雖以企業免責作結，但判決對於個資保護義務認定標準、過失



doi:10.6342/NTU202501770

推定前提、資安制度審查方式及因果關係舉證要求，均提供具體明確的操作指引。此判決形塑了未來同類案件中法院審查責任成立與否的邏輯框架，亦突顯企業應強化制度執行與證據保存的重要性。未來在個資外洩案件日益增加的趨勢下，此判決有助於實務確立一套較為平衡的責任判準，在保障消費者權益與維護企業正當防禦之間取得制度性的穩定性。

## 第三項 雄獅旅行社股份有限公司 108 年個資外洩案

裁判字號：臺灣士林地方法院 108 年度湖小字第 558 號民事判決

一、案件事實

(一) 原告起訴主張：原告主張其於 105 年 5 月至 106 年 8 月間，陸續於被告雄獅旅行社八德門市購買機票，並於 106 年 8 月 19 日下午 3 時許以信用卡方式完成交易。惟於當日晚間 7 時許，即接獲冒稱被告會計人員之詐騙電話，指稱因門市作業疏失誤設分期扣款，需原告配合處理。原告信以為真，依詐騙者指示前往提款機操作，最終匯款 4 萬 187 元至第三人帳戶，蒙受實質財務損失。原告並指出，被告雄獅旅行社早於 106 年 5 月即發生個資外洩事件，卻未採取補救措施或強化資安防護，致於同年 8 月再次發生其個人資料遭不法利用之情事。原告認為，被告雄獅旅行社未盡個資法所要求之安全維護義務，構成違法處理個人資料，並間接促成詐騙事件之發生。基此，原告援引個資法第 29 條第 1 項，請求法院判令被告雄獅旅行社賠償 4 萬元之損害。

(二) 被告雄獅旅行社抗辯：被告雄獅旅行社主張，其於 106 年 5 月遭境外駭客入侵後，已即時報案並委請資安顧問強化防護措施，包括提升加密等級與安全管理。針對近四個月內消費者，亦透過簡訊、電話、網站與門市公告等方式反覆提醒防詐資訊，明確聲明不會以訂單錯誤或分期設定等理由要求匯款或提供帳戶資料，原告亦曾多次接獲簡訊提醒。被告雄獅旅行社已盡資訊安全與告知義務，並無違反個資法。原告未能舉證證明被告雄獅旅行社違法，且其損害係因未查證即信任詐騙電話，自行匯款所致，與被告雄獅旅行社間不具相當因果關係，應自負其責，請求駁回其請求。



doi:10.6342/NTU202501770

二、法院判決理由[79]

本案原告主張因個資外洩遭詐騙而受損，被告雄獅旅行社未善盡個資法之安全維護義務，應負損害賠償責任。惟法院審酌後認為，原告之請求不符損害賠償之構成要件，判決駁回原告之全部請求，理由如下：

(一) 原告未能證明其個資係由被告洩漏，故不得認被告雄獅旅行社違反個資法第27條之安全維護義務：法院指出個資法第27條規定非公務機關保有個人資料者應採取適當安全措施，若違反致資料外洩並損及當事人權利，即原則上須負損害賠償責任，惟能證明無故意或過失者得免責。法院進一步援引最高法院判例，說明如係主張自身權利受侵害者，仍須就有利於己之事實負初步舉證責任。本案中，儘管被告雄獅旅行社承認網站系統曾於106年5月遭到境外入侵，但並無證據顯示原告個資確實因此次事件而外洩，亦無法確認詐騙者所使用之資訊即來自該入侵事件。原告未能具體提出該等資料流出之證據，僅以推測或時間接近作為主張依據，法院認為無法證明其資料係由被告雄獅旅行社處洩漏，因此不構成個資法第27條所稱之違法蒐集、處理或洩漏行為。

(二) 被告雄獅旅行社已於網站入侵後即時以簡訊與電子郵件方式提醒原告，無違反個資法第12條之通知義務：針對原告主張被告未盡資訊外洩後的通知責任，法院指出，個資法第12條及其施行細則第22條已明定公務機關或非公務機關在發現個資被洩漏等情形後，應以適當方式通知當事人，以利其採取自我保護措施。法院審認本案中，被告雄獅旅行社於106年5月23日及26日已向原告發送提醒防詐騙之簡訊，並以電子郵件主旨為「雄獅會員防詐騙說明」通知會員注意資料安全與詐騙手法。該等內容不僅提醒消費者「公司不會要求匯款」、「若有疑問應撥打客服或反詐騙專線」，且方式、時點、文字皆符合施行細則所稱「即時且可得知悉之通知方式」。原告亦不爭執曾收到相關簡訊，故法院認定被告雄獅旅行社已依法盡通知義務，難認其行為有違個資法第12條。

(三) 原告遭詐騙所生之財產損害，與被告雄獅旅行社之行為間不具相當因果關係：

[79] 臺灣士林地方法院108年度湖小字第558號民事判決。



doi:10.6342/NTU202501770

法院進一步檢視原告損害是否與被告行為具備「相當因果關係」，依據最高法院 98 年度台上字第 673 號判決所採「條件理論」與「相當性原則」為標準。即，損害結果須為加害行為不可或缺之條件，且依一般社會經驗，有此行為即足生此結果，始構成相當因果關係。法院雖表示，若被告雄獅旅行社確有疏於維護個資，原告資料因此外洩，或可視為間接原因，但同時指出，被告雄獅旅行社已於事發前三個月多次通知原告應警覺詐騙行為，而原告仍於購票數小時後即依陌生來電指示至 ATM 匯款，係屬個人輕信所致。法院並補充，縱使資料外洩亦不當然導致財產損失之結果，原告受騙並非被告過失所「通常」導致之結果，乃屬偶然之事實，故雙方間不具法律上之相當因果關係。

(四) 原告未能證明違法行為與損害結果間之關聯，請求依個資法第 29 條主張損害賠償，應予駁回：個資法第 29 條規定，當資料當事人之權利因不法蒐集、洩漏等行為受侵害時，得請求損害賠償。但本案中，法院經綜合判斷，認定原告未能提出具體證據證明其個資確由被告雄獅旅行社處洩出，亦未能說明被告雄獅旅行社在安全維護或通知義務上有違失，縱令假設被告雄獅旅行社存在疏失，原告因個人輕信而遭詐騙之行為亦無法歸責於被告雄獅旅行社，雙方間不具賠償所必要之相當因果關係，構成要件未備，依法律不得請求賠償。

(五) 綜上所述，法院最終認定，原告既無法證明個資外洩確係肇因於被告雄獅旅行社，亦難以證明被告雄獅旅行社行為與損害結果間具備相當因果關係，故其依個資法第 29 條提起之損害賠償請求，欠缺構成要件，應予駁回。

三、判決影響與未來發展之分析

(一) 強化舉證責任在個資外洩案件中的防線功能：本案延續傳統民事訴訟舉證責任原則，重申原告作為主張權利受侵害者，應先提出具體事證證明個人資料確實因被告未妥善管理而遭外洩。法院指出，僅憑被告雄獅旅行社系統曾於數月前遭駭客入侵的事實，難以推論詐騙者使用的資料即係該次事件所致。此一標準雖符合法律技術對因果鏈條之嚴格審查，然亦顯現出在數位犯罪日益高度化之情境下，個資主體對資料來源追溯能力的相對弱勢。未來實務若持續依循相同思維，消費者即使明確遭詐、懷疑特定平台資安問題，亦往往難以跨越證明洩漏源的高門檻。此將促使實務在舉證責任上採更細緻分配，或引入推定外



doi:10.6342/NTU202501770

洩的合理懷疑標準，以因應資料流動隱密、犯罪跨境難查之結構現實。

(二) 具體界定企業履行通知義務的合格標準：

1. 判決對個資法第 12 條之解釋亦具實務指引價值。法院肯定被告雄獅旅行社於資安事件後，透過簡訊與電子郵件提醒消費者注意詐騙行為，已達「適當通知」之要件。此一見解有助於釐清實務中企業通知義務之履行界限，表明：即使未能個別確認資料是否遭竊，只要在合理懷疑資料遭侵害之際，企業即應以足以讓消費者知悉的方式傳達風險資訊。此舉亦可鼓勵企業建立自動化的危機溝通機制，發生資安事件時即時觸發預警與回應流程，降低被認定違反通知義務的風險。

2. 然而，本案亦突顯現行制度之不足，即當企業面對大規模資料處理責任時，法院對其「通知義務」之要求仍偏重形式層次，如通知方式是否傳達，而未進一步檢視企業在風險認知、資料存取控管、回應速度等「實質治理措施」上是否合乎合理標準。未來實務與立法應考量將第 12 條義務與第 27 條「安全維護」義務連動解釋，提升企業整體資安風險治理水準，而非僅停留於通知作業之表面形式。

(三) 嚴格定義因果關係限制了對資訊侵害的實質補救：

1. 最具爭議者，莫過於法院對於「相當因果關係」的狹義認定。即便被告雄獅旅行社系統確有曾遭入侵之紀錄，法院仍認為資料是否外洩並無直接證據，且即使發生外洩，亦不當然導致被害人遭詐財損。法院將原告信賴詐騙電話之行為解釋為「個人輕信與疏失」，從而排除被告雄獅旅行社之因果責任。此判斷標準再次突顯資訊時代法律責任認定之困境：在高度仰賴平台與數位交易的生活樣態下，個資洩漏對消費者行為影響深遠而難具體證明，卻反而成為法院否定因果責任的依據。

2. 對照歐盟 GDPR 第 82 條實務中對於「精神損害」、「資料控制者過失」與「可預見性」之寬認，我國法院仍採高度形式證明與傳統過失—因果結構。未來若要提升個資法第 29 條作為實質救濟制度的功能，勢必應在「相當因果關係」之認定標準中引入風險社會之集體性推定邏輯，結合資料流向稽核機制與舉證責任調整，實現真正可及的損害回應制度。



doi:10.6342/NTU202501770

(四) 提醒消費者仍需自我防詐意識，法院亦不全然放寬保護門檻：值得注意的是，法院雖未支持原告請求，惟其理由非全然排除企業應負資安責任，而是強調原告未具體證明洩漏來源與財損間關聯，且曾接獲防詐簡訊仍誤信來電。此亦反映出法院認為企業雖應提供合理防護與告知措施，惟消費者自身在面對詐騙風險時仍應具備警覺義務。這種責任分擔式的判斷，未來仍可能在類似案件中持續適用。

(五) 綜上所述，本案判決提供實務操作中對個資外洩案件法律責任認定的重要參考範式，特別是在舉證責任、通知義務與因果關係等面向給予明確詮釋。未來制度改革方向，應從建立企業資安問責體系、完善外洩舉證工具、引入因果推定與集體救濟機制著手，以回應數位環境中消費者資訊權益保護的迫切需求。

## 第四項 王品瘋美食 App 個資外洩案

裁判字號：臺灣臺中地方法院 110 年度中簡字第 1952 號民事判決、臺灣臺中地方法院 112 年度簡上字第 120 號民事判決

一、案件事實

(一) 原告起訴主張：原告於 100 年間即在被告王品王品餐飲股份有限公司（下稱王品公司）集團旗下「西堤牛排」官網註冊成為會員，並自 109 年間起透過整合後之「王品瘋美食 App」（下稱系爭 App）持續使用會員服務。109 年 11 月 19 日，原告於系爭 App 平台進行會員訂位，並至西堤牛排新店民權店實際消費，完成一筆信用卡付款交易。嗣於 110 年 3 月 6 日接獲自稱為西堤餐廳來電之詐欺電話，來電者能詳實說出原告於 109 年 11 月的實際消費細節，佯稱因系統錯誤產生 20 筆扣款，誘使原告誤信並依其指示進行匯款，共遭詐騙 99,996 元。原告認為詐騙集團得以準確掌握其個人資料與交易紀錄，實係因被告王品公司未妥善管理其透過系爭平台所蒐集、處理及利用之個人資料（包括姓名、聯絡資訊、生日、信用卡資訊、用餐紀錄等），致使系統存有資安漏洞，而使原告個資外洩，終為詐騙集團所利用。原告依據下列法律關係提出請求法院判命被告王品公司給付損害賠償 509,988 元，及自起訴狀繕本送達翌日起至清償日止，按年息 5%計算之利息。



doi:10.6342/NTU202501770

1. 個資法第 27 條、第 29 條：被告王品公司未善盡個資保護之安全維護義務，構成違法，應負損害賠償責任。
2. 民法第 184 條侵權行為責任：被告王品公司之個資外洩行為與原告財產損失間具相當因果關係，應認係與詐欺行為具有幫助關係之共同侵權人。
3. 消費者保護法第 51 條：系爭平台為消費契約基礎，被告王品公司應依消保法對資訊安全與誠信交易負責，並應負二倍懲罰性賠償。
4. 王品瘋美食 App 會員契約：基於契約義務不完全履行，被告王品公司亦應負損害賠償責任。
5. 民法第 172 條無因管理規定：被告西堤餐廳洩漏原告消費交易紀錄，主觀為原告利益，客觀管理原告事務，屬無因管理行為。

(二) 被告王品公司抗辯

1. 否認個資外洩與自身有關，亦無過失：被告王品公司否認原告之個人資料係自其公司外洩。主張現今電子交易涉及多方參與者，包括信用卡發卡行、交易平台、第三方支付或電信應用程式等，詐騙集團得以取得資料之管道甚多。原告曾於郵局 APP 或中國信託信用卡等管道進行交易，無法排除其他來源之可能性，原告僅以其被騙事實推論個資由被告王品公司洩漏，於法並不足採。即便假設被告王品公司遭駭導致個資外洩，亦應認被告王品公司為受害者而非加害者，最終造成原告財損者，係第三人詐騙集團之故意犯罪行為，被告王品公司並無參與、控制或幫助，兩者間欠缺相當因果關係。
2. 原告自身具重大過失：原告於 110 年 3 月 6 日接獲詐騙來電時，對方雖能詳述原告消費細節，惟其仍未提高警覺，反而在詐騙集團之指示下，依序操作郵局 APP、填入異常金額進行轉帳，顯示其有疏忽之舉。尤其在被告王品公司早於 2 月底及 3 月初即透過臉書、LINE 簡訊等管道發布多則防詐騙警示，原告應可合理預期此類風險，其未採取防範措施，應認為對於損害發生與擴大具有重大過失，依民法第 217 條第 1 項，被告王品公司得因此免除或減輕賠償責任。
3. 消保法不適用於個資保護爭議：被告王品公司進一步主張，餐飲服務屬一次性消費，會員制度與個資蒐集屬附隨性質，並非營業項目之本體。消費行為應以



doi:10.6342/NTU202501770

原告實際至餐廳用餐、付款之行為為限，其註冊成為會員、領取生日優惠或接收行銷訊息並非收取對價之服務提供，因此不構成消保法第 7 條所稱之「商品或服務」。即使有會員服務約定或 App 功能提供，原告所稱個資爭議仍應屬個資法所規範之事項，依特別法優於普通法原則，不應逕援用消保法上無過失責任或懲罰性賠償制度。否則將導致加害者（詐騙集團）無責，被害人可逕向無過失之公司請求多倍賠償，結果顯失公平，並違背個資法制度設計。

二、法院判決理由

(一) 一審判決[80]

1. 被告王品公司並無幫助詐欺集團詐欺原告而有共同侵權行為，原告依侵權行為法律關係請求被告王品公司賠償，並無理由：法院認為，原告雖主張被告王品公司因資安疏失導致個資外洩，使詐騙集團得以掌握其消費細節進行詐騙，應屬侵權行為的幫助人，與詐騙集團構成共同侵權。但法院依據民法第 184 條及最高法院判例，強調損害賠償之成立需具備侵權行為之成立要件，包括加害人之故意過失、不法性、損害結果及因果關係，且由原告負舉證責任。法院指出，即使個資是自被告王品公司洩出，亦無從直接推論被告有意圖幫助詐騙集團，因詐騙集團係獨立第三人犯罪行為，其行為非被告王品公司所能控制，被告亦無共謀、參與詐騙之情況。法院進一步強調，社會上一般交易行為不當然構成不法行為，原告未能證明被告王品公司行為具備不法性或與損害間有相當因果關係，故此部分侵權行為損害賠償請求無理由。

2. 被告王品公司確有未採行適當之安全措施，以防止其保有之原告消費個資被竊取或洩漏，而有違反個資法之事實：法院認定，被告確有違反個資法第 27 條與第 29 條之情事，未妥善採取安全措施，導致原告消費資料遭竊取並被詐騙集團利用。法院根據 165 反詐騙平台資料及相同時間其他消費者在被告粉專反映被詐騙之留言，認為可合理推定原告個資即係自被告王品公司平台流出，並非信用卡機構或其他來源。被告王品公司雖主張資訊外洩可能另有他途，然未具

[80] 臺灣臺中地方法院 110 年度中簡字第 1952 號民事判決



doi:10.6342/NTU202501770

體舉證說明其他來源具體為何，抗辯無據。再者，法院指出被告王品公司未能證明自身已採行適當資安措施或無故意過失，反而證據顯示其事後才補發反詐通知訊息，未即時警示原告，亦未盡善管理義務。法院依個資法第 28 條第 2 項之推定規定，認定被告王品公司應對原告非財產損害負賠償責任，酌認賠償慰撫金 2 萬元。

3. 原告依契約及消保法之相關規定，請求被告王品公司賠償，並無理由：法院認為，消保法第 2 條所稱「消費關係」，係指以消費為目的進行商品或服務交易之法律關係。原告主張系透過被告王品公司之 App 訂位並獲取會員優惠，應屬消保法保護對象，並依此主張雙倍懲罰性賠償金。但法院指出，App 會員個資之保管本質上並非被告王品公司收取對價所提供之服務，亦非其營業主體活動，而僅屬促銷性質之附隨資訊服務。故 App 平台使用與個資保管行為非屬消保法第 7 條「商品或服務」範疇，應以個資法為特別法處理。若依原告主張適用消保法第 51 條懲罰性賠償制度，反將使個資法制度架空，亦使被告王品公司須負較詐騙集團更重責任，有違衡平。因此，法院認定消保法與會員契約所生之懲罰性損害賠償請求無理由。

4. 原告依無因管理之法律關係，請求被告王品公司賠償，並無理由：法院指出，民法第 172 條與第 173 條所規定之無因管理，係指在未經本人授權或委任之下，管理他人事務，並須符合「主觀為他人利益」與「客觀有利於本人」等要件。原告主張其消費資料遭被告王品公司蒐集與保管，被告王品公司即負有保護義務，倘個資洩漏則應負無因管理責任。法院認為，本案原告與被告王品公司間實有契約關係，消費資料之提供與保管係基於會員契約或 App 使用條款所生，屬雙方間有法律上原因之行為，不構成無因管理。既有契約關係存在，自無從適用無因管理之規定請求損害賠償。原告於此部分主張顯屬誤會，法院予以駁回。

5. 一審判決被告王品公司應依個資法賠償非財產損害 20,000 元，並自 110 年 4 月 7 日起至清償日止，按年息 5%給付利息。原告其餘請求（財產損害 99,996 元、懲罰性賠償、無因管理）均駁回。



doi:10.6342/NTU202501770

(二) 二審判決[81]

1. 個資法與民法之責任構造與舉證責任：法院首先說明個資法的基本立法目的，係在於保障個人資料所衍生之人格權利，並促進個資的合理利用與安全管理。依據個資法第 12 條、第 27 條及第 29 條之規定，非公務機關若違反安全維護義務，導致個資遭竊取、洩漏、竄改等侵害，即原則上須負損害賠償責任，惟得以舉證無故意或過失抗辯。此責任構造屬於「過失推定」制度，受害人不需證明企業有過失，而是由企業負舉證責任證明其並無過失。然法院進一步指出，即便適用過失推定原則，受害人仍需就其個資「實際遭到不法蒐集、處理、利用」等事實負舉證責任。此外，民法第 184 條亦為請求基礎之一，法院認為個資法構成民法一般侵權行為的特別規定，二者應合併適用，須具備損害、責任事由與相當因果關係，方能成立賠償之債。此段落奠定法院對本案法律適用與責任認定的基本方法論，並強調即使個資疑似外洩，原告仍須就不法利用及損害間之因果連結具體舉證。

2. 消費行為與詐騙事件之事實認定：法院對原告之主張及提出證據加以逐一檢視，確認其於 109 年 11 月 19 日確曾以個人資料註冊「王品瘋美食」APP 會員並完成西堤牛排新店民權店之訂位與刷卡付款，當日消費金額 4,185 元，均透過「瘋 PAY」線上支付功能完成。嗣後於 110 年 3 月 6 日晚間，原告接獲自稱為西堤店員來電，對方能明確說出前次消費金額、時間、細節等資訊，並虛構重複訂單理由，誘導其依指示分別匯款至指定帳戶，合計損失 99,996 元。原告並提供會員資料、點數紀錄、網路訂位憑證、報案紀錄與匯款證明等，法院據此認為詐騙過程具體、連貫且具備可信度，加上被告王品公司對該消費紀錄亦未爭執，故法院認定原告消費資訊確實儲存於被告王品公司之平台，並被詐騙集團掌握並利用行騙，資料外洩情事可受信。因此，法院承認事實基礎成立，惟後續是否能歸責於被告王品公司，尚需從過失與因果關係角度進一步審視。

3. 被告王品公司是否違反個資法安全維護義務：法院首先肯定被告王品公司確實

[81] 臺灣臺中地方法院 112 年度簡上字第 120 號民事判決。



doi:10.6342/NTU202501770

透過自家 APP 平台儲存消費者之姓名、聯絡方式與交易紀錄等個人資料，依個資法第 27 條，被告王品公司負有採行「適當安全措施」防止資料洩漏之法定義務。原告主張其個資遭駭客竊取並提出與客服、店經理之對話記錄、報案資料及同類型詐騙案件新聞為佐證，指稱被告王品公司之平台資安不足導致個資外洩。然法院進一步檢視被告王品公司實際作為後，認為其已於詐騙事件發生前陸續透過官網、粉絲頁、LINE 推播等管道進行防詐宣導，亦於案發翌日主動發送提醒簡訊。技術面上，被告王品使用遠傳提供之雲端運算服務，具 ISO 27001 國際資安認證，並有硬體防火牆與入侵防禦機制，且消費紀錄資料採加密、隱碼處理。法院據此認為，現有證據難以證明被告王品公司未盡個資安全維護義務，亦無足夠事證可證其對資料外洩或未即時通知原告有所疏失，無違個資法第 12 條、第 27 條規定。

4. 是否成立損害賠償責任與相當因果關係：法院於本段落重點審酌「損害是否為可歸責於被告王品公司之結果」，並聚焦於相當因果關係的判準。法院承認原告確實於詐騙過程中因誤信不實來電而陷於錯誤，導致財產損失，惟該損失係由第三人詐欺集團所故意為之，不屬被告王品公司主體行為。即使假設個資來源為被告王品公司平台，但若無該第三人主動行騙，原告並不會產生匯款行為與損害結果。法院並引用刑事附帶民事判決，指出原告已就詐騙案向該集團成員提告並獲判確定賠償 99,996 元，已獲填補，間接證成損害係由詐欺行為直接導致，與被告王品公司之行為間不具備法律上「相當因果關係」。法院藉此強調：即便企業資料遭不法取用，若無證據證明企業過失與損害結果間存有法律上密切連結，則難以成立侵權損害賠償之請求。

5. 關於消費者保護法之適用與懲罰性賠償請求：法院於此部分否定消保法第 51 條懲罰性賠償之適用。其理由首在於交易關係已於 109 年 11 月完成，至詐騙事件發生時，雙方間不再具備消費關係，因而難以構成消保法第 2 條所稱「消費關係」。其次，法院指出即便構成消費者身份，原告亦未能舉證被告王品公司對詐騙事件有故意或重大過失，未符合懲罰性賠償之要件。此外，法院進一步指出被告王品公司在詐騙事件發生前已發布多則警示資訊，已採取合理預防措施，且無違反消保法第 7 條保障消費者安全之規定。由此，法院認為原告所請求的 199,992 元及 140,000 元懲罰性賠償金於法律上並無依據，難以准許。



doi:10.6342/NTU202501770

6. 法院綜上所述，認為原告主張雖具同情基礎，然無法舉證證明被告王品公司在個資管理上存有違法或疏失，亦無法證明其受害結果與被告王品行為間具備相當因果關係。此外，被告王品公司已依資安標準採行適當防護機制，並於詐騙前後發布多次警語，並無違反個資法第 12 條、第 27 條或消保法第 7 條規定。故法院駁回原告依個資法、民法與消保法提出之財產損害、精神慰撫及懲罰性賠償請求，全案金額 509,988 元均為無理由。更進一步，法院認為原審認定被告王品公司應支付精神慰撫金 2 萬元並准宣告假執行，亦屬未洽，應予廢棄。最終改判被告王品公司完全免責。

三、判決影響與未來發展之分析

本案係關於消費者鄧佩君於王品集團旗下「瘋美食 APP」註冊會員後，其個資疑似遭外洩致使詐騙集團得以取得其消費紀錄並實施詐術，造成財損 99,996 元。原告遂依個資法、民法、消保法及無因管理等多重法律依據請求損害賠償共計 509,988 元。一審判決王品公司應賠償精神慰撫金 2 萬元，二審則改判王品公司完全免責，駁回全部請求。

(一) 法律認定方式之轉變與「過失推定」制度的界限：一審法院根據個資法第 27 條、第 29 條，認為被告王品公司未盡適當安全維護義務，推定其有過失，應對原告所受非財產上損害負賠償責任。此舉顯示法院將個資法視為具有「特別侵權責任」性質，並據以引動民法第 184 條以下侵權規定。然而，二審法院則更為嚴格地詮釋個資法第 29 條之「過失推定」規則，強調該制度僅於原告已證明其個資實際遭不法蒐集、處理、利用之情況下，始能轉換舉證責任至企業。換言之，過失推定並非全然免除原告舉證責任，而仍須針對事實基礎建立「外洩源於被告」的基本證明。二審因此否定一審在客觀要件與主觀要件之雙重推定，認為此舉將個資法誤解為近乎「無過失責任」，有違法制設計。本案即反映出法院對於「個資外洩即為企業可歸責」的推定界線採取收縮立場，亦可視為對企業保護機制的強化，避免將個資法第 29 條擴張至事實未明的情況。此舉雖有助於避免濫訴風險，但亦引發是否會反向削弱個資權保障機制之疑慮。

(二) 相當因果關係的判準與詐騙介入責任切割：在因果關係的判斷上，一審對於詐騙集團取得個資來源雖無直接證據，仍採「合理推定」方法，從 165 反詐平台



doi:10.6342/NTU202501770

報告、同類型留言及被告王品公司遲未通報等綜合情狀推斷外洩來源應為被告王品公司之平台，並據此判定資料保護不當與原告受害間具因果關係。相對而言，二審法院採取更為嚴格的相當因果關係審查標準。法院認為，即使假設資料來自被告王品公司之平台，詐騙行為屬獨立第三人之故意犯罪，非企業可預防與控制。詐騙結果與企業資訊處理行為間欠缺法律上可歸責之緊密聯結，且原告亦已就該詐騙提告，獲刑事及民事判決確定補償，難認被告王品公司應負再度賠償責任。此種見解對於未來類似案件意涵重大。法院事實上是在資訊遭竊與財損發生之間切出「行為鏈斷裂」，明確界定企業資訊管理義務與詐騙犯罪結果之間不可自動連結，將侵權損害責任歸屬於「真實加害人」，而非資料控管者。此亦反映我國法院傾向於維持侵權責任「最小必要擴張」的穩健路線。

(三) 消保法適用之限縮與個資法的特別法定位：一審法院明確指出，王品 APP 提供會員優惠等資訊功能，屬促銷性質之附隨服務，並非消保法第 7 條所稱之「商品或服務」。若以此作為懲罰性損害賠償之基礎，將導致個資法作為特別法之體系遭架空，責任分配亦有失衡之虞。二審則進一步否定「消費關係之延續性」，指出原告消費行為已於 109 年 11 月完成，至 110 年 3 月詐騙發生，雙方間已無現存交易關係，因此難以成立消保法第 2 條所保護之消費者地位。法院重申應尊重個資法為專屬處理個資事件之立法位階，避免雙軌規範導致解釋混亂。此種限制性解釋雖維護法律體系之明確性，但在平台服務已與消費者日常交易緊密結合、資料持續利用之現況下，過度劃定「交易終止即保護終止」的標準，是否仍符合消費者實質風險控管與法律期待，值得持續討論。

(四) 實務運作影響：證據門檻與平台自保義務的再界定

本案對於未來個資外洩案件實務運作有三大影響：

1. 證據門檻大幅提高：法院明確要求原告需就個資「確實外洩」及「由特定企業外洩」負起初步證明責任，僅有社群留言或新聞報導等「間接佐證」難以成為可採基礎。此一舉證標準將使多數無法進入企業內部取得資料流程證據的消費者陷於舉證困境。

2. 平台需建立「可證明之合規機制」：本案中王品提出其使用 ISO 27001 資安認



doi:10.6342/NTU202501770

證、加密隱碼技術、即時簡訊警示、雲端防火牆紀錄等資訊，作為反證其「已盡合理注意義務」的證據，最終成功免責。未來企業若能建立完整合規文件與即時應變紀錄，將成為舉證防線的關鍵。

3. 司法審查重點移轉至「系統性缺陷」證明：若無明確駭客入侵紀錄或外洩溯源證據，法院傾向採無責立場。消費者如欲請求賠償，恐需借重刑案移送調查、聯合訴訟或行政裁罰資訊，以證明平台存在「系統性疏失」或多次類似個案。

(五) 雖然王品 APP 個資案最終以企業勝訴作結，惟該判決實質上凸顯我國現行個資法在實務運作上的三大制度瓶頸，包括證據取得困難、責任判斷技術落差以及救濟效果不足。尤其在數位服務日益普及、資料集中化趨勢下，若仍維持高度舉證責任與嚴格的相當因果關係認定標準，將使消費者在個資外洩與詐騙風險事件中處於極為不利地位。為實質強化個資保護體系，未來制度改革應考慮導入「外洩推定制度」，針對集中持有個資之平台業者，賦予其對外洩不存在負有舉證責任；同時鼓勵發展資料流向追蹤與稽核技術機制，作為法院判斷資料來源與歸責事實之佐證依據；此外，亦應重新檢討平台提供之資訊性附隨服務是否應納入消保法「商品或服務」定義範疇，使消費者得以援用消保法保護與救濟，補足現行個資法於平台型消費關係中之保護缺口。

## 第五項 北投麗禧溫泉酒店股份有限公司個資外洩案

裁判字號：臺灣臺北地方法院 111 年度訴字第 5578 號民事判決、臺灣高等法院 112 年度上字第 656 號民事判決

一、案件事實

(一) 原告起訴主張：原告於 109 年 10 月至 110 年 11 月間，委由他人使用被告北投麗禧溫泉酒店股份有限公司（下稱麗禧公司）所設線上購券系統（下稱系爭訂購系統），購買溫泉券共計 37,300 元，並於訂購過程中提供姓名、電話、電子郵件及信用卡帳號等個人資料。該系統係由被告墨攻網路科技股份有限公司（下稱墨攻公司）建置與維護。原告指控，被告雙方作為非公務機關，並未依個資法第 27 條規定，於蒐集個資後採取適當安全維護措施，致原告個資透過系統遭第三人不法竊取。且被告麗禧公司早於 110 年 11 月底即已知個資外



doi:10.6342/NTU202501770

洩情形，卻未依個資法第 12 條通知原告，未盡事後告知及通報義務。原告於同年 12 月 21 日接獲冒用麗禧名義之詐騙電話，誤信其為客服人員，配合操作致遭詐損失金額 9 萬 9,987 元。因此，原告依據個資法第 29 條第 1 項、民法第 184 條第 1 項前段及第 2 項、第 185 條，請求兩被告連帶賠償財產與非財產損害合計 11 萬 9,987 元及利息，並依個資法第 3 條、第 11 條第 3、4 項，聲明請求兩被告刪除原告留存於系統內之個資，並停止蒐集、處理與利用。

(二) 被告抗辯

1. 缺乏因果關係與外洩來源不明：被告麗禧公司主張，原告遭詐騙時間距離其最後一次於系爭訂購系統購券已近兩個月，期間原告亦曾使用中信銀行信用卡付款，而信用卡公司本身亦可能掌握原告姓名、聯絡方式與交易資訊，難以認定原告之個資即係從系爭訂購系統外洩。原告未能舉證詐騙集團所使用之個資即來自於麗禧公司或墨攻公司所管理之系統，構成舉證不完全。

2. 已採適當資安防護措施：被告麗禧公司早於個資外洩傳聞發生之前，即已投入大量資源升級系統安全，包括提升硬體設備、更新資訊系統及防火牆，並對顧客資料進行加密處理，已善盡個資法第 27 條所要求之安全維護義務，並無故意或過失。

3. 原告與有過失，並無相當因果關係：即使詐騙事件與系爭系統有關，被告麗禧公司已於 110 年 8 月 28 日於官網公告詐騙手法及張貼提醒標語，提醒消費者提高警覺。原告曾多次登入官網，應已知悉該警示，卻仍輕信自稱客服來電，未經查證即配合操作。故其財產損失係原告之輕率行為所致，與被告麗禧公司所為無相當因果關係，縱認被告應負責，原告亦有重大過失，應減免賠償責任。

4. 個資已刪除，無繼續使用情形：被告麗禧公司已依原告要求刪除其個資，僅保留電話號碼用以推播反詐騙簡訊，該資訊並不足以識別個人，無違個資法上使用限制，亦無再刪除之必要。



doi:10.6342/NTU202501770

二、法院判決理由

(一) 一審判決[82]

1. 舉證責任之轉移與減輕：法院首先指出，依民事訴訟法第 277 條但書規定，若將舉證責任分配予原告顯失公平，可酌予減輕。考量本件中系爭訂購系統非原告可見或管理之領域，法院認為原告無須就系統如何被入侵具體舉證。經查，原告確實曾使用該系統並輸入個資，該資料亦儲存於被告麗禧公司資料庫中。證人證述與中華電信通信紀錄顯示，詐騙電話中對方能明確指出原告曾購買之商品與會員身分，與系統儲存資訊相符。另根據交通部觀光局提供之監督通報紀錄，被告麗禧公司於 110 年 11 月 16 日即接獲系統異常入侵通報，估有 5,423 筆個資外洩，時間上與原告於同年 12 月 21 日接獲詐騙電話相當接近。法院綜合前述事證，認為雖原告無法具體證明自身資料為被外洩資料之一，但已足堪信該詐騙行為所依憑之個資即為自系爭訂購系統所竊，故採認原告之主張。

2. 被告已採取適當安全維護措施而無過失：法院審查個資外洩是否可歸因於被告之故意或過失。依個資法第 27 條，非公務機關對所保有個資應採適當之安全措施，否則於資料外洩時應依第 29 條負損害賠償責任。第 29 條第 1 項但書進一步明定，若資料外洩，則被告主張無故意或過失者，應負舉證責任。法院認為本案中被告麗禧公司已完成資安義務，於事前進行 Fortify 掃描未發現高風險弱點，系統亦有數位簽章保障；事發後即委由第三方資安公司進行滲透測試，結果未顯示系統異常；主管機關如數位部與觀光局調查後亦未認定被告違反法定資安義務。綜上，法院認定被告麗禧公司已採適當安全措施，無故意或過失，不符合賠償責任之構成要件。

3. 原告主張其因遭詐騙而受財產損害 99,987 元，並請求精神損害賠償 2 萬元。惟法院既認定被告對個資外洩無過失，損害賠償請求即欠缺違法性與過失構成要件，難以成立。即使原告確有財產及非財產上損害，亦因無法歸因於被告違法行為而不具請求基礎。

---

[82] 臺灣臺北地方法院 111 年度訴字第 5578 號民事判決。



doi:10.6342/NTU202501770

4. 原告援引個資法第 11 條，請求刪除並停止利用其個資。對麗禧公司部分，法院確認原告已於 111 年 1 月 4 日明確表達不同意持續利用其個資。儘管麗禧公司聲稱已刪除部分資料，但仍保留原告電話號碼。法院指出，電話號碼屬個人資料，應依原告意願刪除並停止使用，故命被告履行其法定義務。至於系統建置廠商墨攻公司部分，法院認為原告未能證明其資料仍儲存於墨攻系統，且墨攻公司亦提出查詢結果顯示未保有原告個資，因此駁回原告對其之請求。

5. 綜上所述，法院雖肯認原告個資係由系爭系統外洩，但因被告已盡資安維護義務，對於個資外洩無故意或過失，賠償請求不符個資法第 29 條之構成要件，應予駁回。惟針對資料刪除部分，原告請求有其法律依據，法院予以一部認可。

(二) 二審判決[83]

1. 原告個資為系爭訂購系統外洩所得，舉證已屬充分：法院指出，雖原告對其個資外洩來源須負舉證責任，但因系爭訂購系統由被告建置與管理，且相關證據偏在於被告一方，應適用民事訴訟法第 277 條但書，減輕其舉證責任。原告確實曾多次透過系統購買溫泉券，並輸入姓名、電話、銀行帳號等個資；詐騙集團於電話中自稱為麗禧公司員工，清楚掌握原告購買記錄與身分資訊，顯與系統所留資料一致。根據交通部觀光局回函與通報紀錄，被告墨攻公司所管理的系統於 110 年 11 月遭駭客入侵，預估有 5,423 筆會員資料外洩，時間上與原告於同年 12 月 21 日接獲詐騙電話極為接近。被告所提數發部函文僅稱「無法排除其他可能性」，並未明確否定系統為外洩來源。法院因此認定，原告之個資確係自系爭訂購系統外洩，原告已盡舉證責任。

2. 被告未盡適當資安維護義務，對個資外洩具過失：依據個資法第 27 條，非公務機關應就所保有之個資採取適當安全措施。法院指出，本案中墨攻公司與麗禧公司皆未能提出具體、可驗證之資料以證明其於外洩發生前即已妥善管理系統。被告雖提出多項截圖與政策文件佐證，但多為事件發生後所建立，且資料多經遮蔽，無法確認是否針對系爭系統施作。其所提出之資訊安全政策內容多

[83] 臺灣高等法院 112 年度上字第 656 號民事判決。



doi:10.6342/NTU202501770

為抽象性描述，欠缺具體實作證據。即便交通部與數發部函示認為事後應變尚稱妥適，法院仍認該等意見不具法律拘束力，應由法院獨立判斷。法院據此認定，被告墨攻公司未妥善管理系統，構成過失；被告麗禧公司作為資料擁有者亦未善盡監督義務，雙方皆違反個資法第 27 條規定。

3. 財產損失與被告行為間不具相當因果關係：法院認為，即使被告有資安管理過失，且原告個資確實外洩並遭詐騙集團利用，但財產上損害係由第三人實施詐騙行為所致。所謂相當因果關係，須為在一般經驗法則下，高度蓋然會發生相同結果的條件，而非僅係事實上之條件。本案中原告損失 9 萬 9987 元，為詐騙集團透過社交工程誘導轉帳所致，無法認為係資安疏失在一般情形下必然產生之結果。交通部通報亦載明外洩 5423 筆資料中，僅一件為財產損害案件。因此，原告主張被告應就財產損失負賠償責任，法院認定兩者間不具相當因果關係，駁回其財產損害部分之請求。

4. 原告請求非財產損害賠償成立，金額 2 萬元為適當：法院認為，因被告未妥善保護個資，導致原告之隱私與資訊自主權遭受侵害，構成個資法第 29 條第 1 項與第 28 條第 2 項所指情形。原告主張在遭遇詐騙事件後，為申訴而耗費大量時間並承受精神壓力，需長期擔心資料再次被濫用，該等精神損害自屬可採。法院審酌原告年齡、教育程度、經濟狀況與雙方地位、加害程度等因素，認為原告所請求之 2 萬元慰撫金金額適中，應予准許。此外，法院認定被告墨攻公司未盡資安維護義務，被告麗禧公司未盡監督義務，雖過失內容不同，但所生損害相同，依不真正連帶債務原則，應就該筆慰撫金共同負全部給付責任。

5. 原告請求刪除全部個資未獲採，證據不足：原告主張被告仍保有其姓名、電話、地址、Line ID、UUID 等個資，應依個資法刪除並停止利用。然而，法院認為，被告已提出系統操作紀錄及截圖證明，除電話外，其餘資料均已刪除；原告雖主張仍接獲 LINE 與電子發票通知，但依 LINE 官方與發票平台廠商回函內容，該訊息為平台自動發送，非由被告掌控，亦無可刪除機制。法院認為原告未能提出其他直接證據證明被告仍持續利用或保有上述所有資料，故其刪除全部個資之請求無據，不應准許。

6. 法院綜合上開審理結果，認定被告雙方雖對個資外洩具過失，惟未與財損間成



doi:10.6342/NTU202501770

立相當因果關係，故原告之財產損害賠償請求不成立。然非財產上損害部分則予以肯認，核定慰撫金為 2 萬元，並判二被告負不真正連帶責任。至於個資刪除與停止利用之請求部分，因證據不足及屬平台設定事項，亦予以駁回。故全案判決結果為「一部有理由，一部無理由」。

三、判決影響與未來發展之分析

本案源自原告於北投麗禧公司線上訂購系統購買票券並輸入個資後，接獲詐騙電話而誤信操作，致損失近 10 萬元。原告認為，其個資係由該系統外洩，而系統係由被告麗禧公司與被告墨攻公司共同營運與管理，二者對資安防護與外洩通報義務未盡妥適處置，應依個資法第 29 條與第 11 條負損害賠償與刪除個資之責。一審肯認原告個資係由系統外洩，惟認被告已盡安全維護義務，對外洩無過失，否定損害賠償請求。僅針對被告麗禧公司未刪除原告電話號碼部分，命其限期刪除。二審改變部分見解，認為兩被告確有未盡妥適資安與監督義務之過失，惟仍否定財損與外洩間之相當因果關係，駁回財產損害賠償請求。但對原告資訊自主權受損之精神痛苦予以肯認，酌定賠償 2 萬元，由兩被告負不真正連帶責任。至於刪除 Line ID 與其他個資之請求，則因證據不足而不予採納。

(一) 法院對個資外洩「來源認定」的舉證責任標準明確化：本案在一二審均採肯定原告個資來源係自系爭系統外洩，理由在於法院將個資外洩舉證標準調整為「推論式間接證據認定」，不要求原告提出技術證據或精確資料外洩鏈，而是透過以下綜合判斷：原告曾使用系統、詐騙話術內容與原購資料吻合、官方紀錄載明系統遭駭、時間序近等。此舉有效緩解個資案原告面對「舉證困難」的制度性弱勢，亦使實務逐漸走向「外洩源之事實認定可經常理推定」的標準，有助於未來同類案件的起訴與審理效率提升。

(二) 「外洩不等於過失」之責任界線獲具體展現：本案一審即認為，被告雖資料遭駭，但其已完成 Fortify 掃描、使用簽章控管、事後迅速檢測，且獲主管機關肯認無資安疏失，不具過失責任。二審則對此部分進行更細緻的實質審查，指出被告提出之資安憑證多為事後補強，事發前並未具體落實資料防護政策與查核機制，構成個資法第 27 條所稱之「未盡適當安全措施」過失。此一認定意謂：即使業者系統遭駭，不代表一定有過失，但若資安管理缺乏可驗證之內



doi:10.6342/NTU202501770

控機制，將仍可能構成法律責任。該判斷精準區分「不可抗力型外洩」與「制度性疏失型外洩」，補強了現行個資法第 29 條過失認定之裁量技術。

(三) 因果關係認定仍以「高蓋然性」為限，財損救濟受限：

1. 法院在肯認個資確實遭駭與遭詐騙利用的同時，仍否定財產損害賠償請求，理由係基於「外洩本身並不必然導致詐騙匯款」之風險鏈條斷裂。法院以交通部資料顯示 5423 筆外洩中僅 1 件涉及財損為據，認為詐騙結果非外洩之自然結果，雙方間不具「相當因果關係」。

2. 此種因果邏輯建構，雖符合理論上區分行為與損害間之可預見性與蓋然性，惟對消費者而言仍存高度不確定性與救濟瓶頸。在數位詐騙日益猖獗背景下，此種判斷可能產生「原告證明責任過重、業者行為門檻過低」的保護落差，亦顯示我國在個資損害因果關係認定仍待引進如「推定連結原則」、「風險負擔反轉」等制度性轉化。

(四) 精神損害賠償的漸進肯認與量化標準雛形：值得注意的是，二審法院肯認原告之非財產損害成立，理由為個資外洩已侵害其資訊自主權、隱私權與安心生活權，構成精神壓力。該判決亦援引原告年齡、身分、主觀痛苦與被告過失程度等因素，酌定賠償 2 萬元。此判斷與過往多數否定非財損害的保守態度相比，具有突破意義。

(五) 個資刪除請求應結合技術實踐與證據呈現：對於原告請求刪除 Line ID、UUID、Email 等資料，法院以「無證據顯示仍持有」及「部分為平台自動推播、非麗禧所控制」為由不予准許，反映目前刪除請求審查仍依賴「證據層級」與「控制範圍」兩項核心。然此亦暴露出現行制度對於跨系統平台、API 資料流通的權責歸屬缺乏技術對應與法律清楚標準，未來若無修法與主管機關指引，將持續形成資料刪除請求落空的常態。

(六) 行政機關意見不具拘束力，民事法院自為認定過失責任：

1. 本案另一值得關注之處，為法院對主管機關（交通部觀光局、數位發展部）所提供之回覆意見採取保留態度。雖兩機關均表示：墨攻公司針對系統外洩事件已依規完成通報，並實施後續修補作業，未認有違反資安責任之虞，然法院並



doi:10.6342/NTU202501770

未直接據此否定過失，而仍就系統原始防護機制是否具體落實、資安政策是否事前建構、舉證內容是否具體明確進行自主判斷。

2. 此種立場顯示法院並不視行政機關意見為「法律上當然有效」之認定依據，而是將其作為佐證之一。司法機關於民事責任判斷中，仍須依據舉證責任分配、過失構成要件、舉證證據之內容與完整性作獨立判斷。此一作法強調司法中立性與審判獨立性，避免行政解釋凌駕法院法律適用。

3. 然而，實務上行政機關與企業之間往往具有資安通報與技術協作的第一線關係，若行政認定與法院判決標準落差過大，恐生企業「合規即不免責」之疑慮。未來制度宜考慮建立明確的資安義務層級與法律推定效果，例如將「主管機關認定無過失」作為可推翻之舉證起點，兼顧法官自由心證與企業可預期性。

(七) 綜觀本案，一二審雖在部分認定上有所差異，但整體展現出個資外洩案件中法院對於「舉證責任配置」、「過失要件精緻化」、「因果關係門檻」及「非財產損害承認」的逐步調整。判決兼顧證據合理性與技術現實，對實務與學理均具啟發性。本案也提醒企業，未來資安責任評價將不僅止於事後應變，更重制度規劃與紀錄留存。對法院而言，則可考慮建構更為系統性之「外洩源推定標準」、「因果風險分擔原則」與「非財產損害評價工具」，以強化數位風險下消費者的程序保障與實質救濟。

## 第六項 中華民國運動神經元疾病友協會個資外洩案

裁判字號：臺灣臺北地方法院 111 年度北簡字第 1007 號民事判決、臺灣臺北地方法院 11 年度簡上字第 266 號民事判決

一、案件事實

(一) 原告起訴主張：被告中華民國運動神經元疾病友協會（下稱漸凍人協會）係社團法人公益團體，日常接受各地善心人士之捐款，其所保存之捐款明細內含姓名、電話、聯絡地址及銀行帳戶等個人資料，應受個資法第 19 條至第 21 條關於目的外利用、資料正確性維護及安全措施之規範。然而，被告漸凍人協會未善盡保管個人資料之義務，導致資料外洩。依新聞報導，被告漸凍人協會於 110 年 7 月 26 日即知悉多間公益團體所委託之網路管理公司（即網軟股份有限公



doi:10.6342/NTU202501770

司，下稱軟網公司）發生個資外洩事件，惟未依個資法第 12 條通知受害人，亦未妥善處理後續個資侵害事宜。原告並主張其於 110 年 8 月 20 日左右接獲詐騙電話，對方冒用被告名義，以處理捐款為由詐取款項。原告因而陷於錯誤意思表示，轉帳 149,987 元，並支付手續費 8 元，合計損失 15 萬 5 元。原告進一步主張，因遭此詐騙致失去家庭半年生活費，並遭受精神痛苦，爰請求被告漸凍人協會給付財產損害賠償 150,000 元及非財產損害慰撫金 10,000 元，合計請求金額為 160,000 元。

(二) 被告漸凍人協會抗辯：

1. 原告起訴內容欠缺明確性，未具體說明其主張損害賠償之法律基礎究竟為何，未釐清係主張與被告漸凍人協會委託之網路管理公司（網軟公司）間構成共同侵權，抑或是因選任、監督失當應負連帶責任，亦未明示其所主張之法益受侵害類型為何。由於原告未盡具體主張之責任，致被告漸凍人協會無從準確作出答辯，嚴重妨害其訴訟防禦權。

2. 縱原告所述部分事實屬實，仍應負完全舉證責任，證明包括：網軟公司確實遭到資料庫入侵；原告個資係因此入侵事件而洩漏；詐騙電話確係利用該等外洩資料與原告聯繫；被告漸凍人協會於 110 年 7 月 26 日起即知悉該外洩情形；被告漸凍人協會對網軟公司確具有實際指揮或監督能力；以及原告之損害與該資料外洩之間具備相當因果關係。惟原告未就上述各項提出具體證據，致其請求根本欠缺事實基礎。

3. 此外，針對原告所引用之新聞報導內容，以主張被告漸凍人協會早於特定日期即知悉外洩事件，然此類報導性質上僅屬傳聞，不具證據能力，且原告所提出之報導內容，並未明確指出被告確有即時得知個資外洩之事實，應無採信之餘地。

4. 被告漸凍人協會與網軟公司僅係委託儲存電子資料與提供技術服務之關係，雙方間並無指揮監督關係存在。就個資法第 12 條所規定之通知義務，亦僅限於非公務機關違法致個資外洩時始適用，而本案並無任何證據顯示被告漸凍人協會有違反個資法之行為，故自不生通知義務之適用。綜合以上各項主張，原告之訴既缺乏具體事證佐證，亦不符法律上之構成要件，應予以駁回。



doi:10.6342/NTU202501770

二、法院判決理由

(一) 一審判決[84]

1. 舉證責任與侵權構成要件的適用：法院首先就民事訴訟中舉證責任的分配加以說明，指出依民事訴訟法第 277 條，當事人對於自己主張有利之事實，應負舉證責任。特別是在侵權行為的案件中，如由原告主張被告行為成立共同侵權者，其有責任就該侵權事實提出具體證據。此外，法院引用最高法院實務見解指出，對於常態與變態事實之舉證標準不同，主張變態事實者（如個資外洩源自特定被告）應負較高的舉證責任。本案中原告即需證明被告確實涉入個資外洩，並與其損害間具備構成共同侵權之條件。

2. 原告未能證明個資外洩源頭及被告行為違法性：針對原告主張其個人資料係由被告漸凍人協會外洩並遭詐騙所利用，法院認為原告僅提出其自身遭詐騙經驗與報導資料為據，未提出任何可具體證明該協會即為資料外洩源的事證。法院指出，該等報導未載明駭客身分、駭入方式及來源，僅屬間接說法，難以採信。即使退一步認為漸凍人協會資安措施不完備，原告亦未指出協會違反個資法之具體條文，僅泛稱應遵守第 19 條至第 21 條，欠缺構成要件。法院進一步分析指出，協會依第 19 條第 5 款取得個資，為經當事人同意，並無違法處理或濫用個資之事實。至於原告所指被駭資料後遭詐騙，實際加害人為駭客，並非協會本身，不符個資法歸責要件。另原告對網軟公司之指摘亦未具證明力，僅證明其提供主機空間，並未負責資料蒐集或處理，自難構成侵權責任。法院最後比附他人之物品遭竊再被用於詐騙第三人，原所有人並無法因詐騙結果負責，說明本案亦屬類此情形。

3. 原告損害請求無事實依據，應予駁回：綜合前述分析，法院認為原告未能舉證證明被告漸凍人協會係違反法定義務或資安規範之加害人，亦無證明其行為與原告損害間具備法律上之相當因果關係。原告雖主張因個資外洩致財損，惟未能建立加害行為與損害結果間之直接聯繫與責任基礎，難認其主張成立。法院

[84] 臺灣臺北地方法院 111 年度北簡字第 1007 號民事判決。



doi:10.6342/NTU202501770

因此認定，原告請求被告漸凍人協會給付 16 萬元之訴訟請求，欠缺構成要件及事實基礎，應予以駁回。

(二) 二審判決[85]

1. 法院對原告匯款事實之認定：法院確認原告於 110 年 8 月 15 日自其玉山銀行帳戶轉帳 15 萬 2 元至訴外人林雅婷所設合作金庫帳戶，依據玉山銀行與合作金庫所提供之交易明細、公文函及新開戶建檔單等證據，加上雙方當事人對此並無爭執，法院認定該筆匯款事實成立。此為後續損害及因果關係判斷的基礎事實。

2. 原告舉證不足與因果關係之否定：

(1) 個資法與民法侵權條款之法律適用說明：法院說明，個資法第 27 條規定非公務機關應採取適當安全措施防止資料外洩，違反者如致損害，可能構成民法第 184 條第 2 項侵權責任。該條為轉介及概括性條款，須引入具體保護他人之法規加以補充適用。法院引用最高法院見解指出，若違反以保護個人權益為目的之法規並導致損害，即推定其有過失，但仍須進一步認定損害與違法行為間具備「相當因果關係」方成立賠償責任。

(2) 法院指出，原告主張其系因個資外洩而遭詐騙匯款，然而並未提出具體證據證明系爭資料確為被告洩漏。法院並檢視原告所引用之網站聲明，內容僅為澄清內部網路安全並提醒捐款人注意詐騙，未顯示協會自認資安疏失。法院並進一步釐清「相當因果關係」須同時具備條件關係與相當性，若僅存在事實上關聯而無可預見性與通常性，則不構成民事責任。

3. 對網軟公司為外洩源頭之否定：原告另主張網軟公司為資料外洩來源，然其所據為公益團體自律聯盟之網路聲明，該聲明雖提及捐款系統廠商資料庫遭駭，但未具體指向被告網軟公司。法院認為該聲明無法直接證明本案所涉資料係由網軟公司保有並外洩，原告亦未能提出任何證據證明網軟公司實際管理或保有其個資。因此，法院認定原告僅據網路聲明臆測，尚難作為訴訟上有利事實之

[85] 臺灣臺北地方法院 111 年度簡上字第 266 號民事判決。



doi:10.6342/NTU202501770

基礎，舉證顯然不足，請求自難成立。

4. 無證違法事實則不得適用個資法第 29 條請求賠償：法院指出，個資法第 29 條與第 28 條第 3 項雖允許當被害人難舉證實際損害時，得以酌定金額請求賠償，惟前提為行為人確有違反保護義務。本案中，原告未能證明被告漸凍人協會或網軟公司違反個資法第 27 條，因此即無從成立法律上請求權之前提條件。法院進一步指出，原告並未具體指明被告違反個資法哪一條款，僅泛稱應依第 19 條至第 21 條處理資料，已難構成具體違法行為之指摘。因此，其請求賠償金額無論定額與否，均不符要件。

5. 法院綜整全案事證後認定，原告無法證明兩被告有違反個資法第 27 條之行為，亦未能證明其匯款損失與被告任何作為間具責任成立所需的相當因果關係。不論原告係依據民法第 184 條第 2 項、第 185 條或個資法第 29 條、第 28 條第 3 項請求損害賠償，均無法律及事實基礎，應予駁回。法院並認原審判決並無違誤，原告上訴意旨亦無理由，故上訴駁回，確定被告不負賠償責任。

三、判決影響與未來發展之分析

本案涉及原告主張其個人資料遭洩漏，因而受詐騙電話誘導，匯出款項導致損失 16 萬元，故向被告漸凍人協會及網軟公司請求損害賠償。然一審與二審法院均認為原告未能提出足夠之證據證明被告違反個資法義務，且原告所主張之損害與被告行為間欠缺法律上所要求之相當因果關係，故駁回原告之請求及上訴。

(一) 舉證責任分配之明確化：本案判決首先凸顯民事訴訟中舉證責任的明確化趨勢。法院援引民事訴訟法第 277 條規定及最高法院實務見解，重申主張有利於己之事實者負舉證責任，尤其在個資外洩案件中，法院更進一步強調主張「變態事實」（如資料外洩源頭指向特定被告）之原告，須負擔較高之舉證義務。此一舉證責任之明確化，未來勢將影響個資外洩案件的訴訟策略，原告須事先蒐集充足證據方能勝訴，避免僅依間接證據或媒體報導作為訴訟基礎。

(二) 相當因果關係審查之嚴格化：法院對於相當因果關係的審查亦十分嚴格，尤其強調「條件關係」與「相當性」必須兼備，方足以認定侵權行為成立。法院明確指出，僅憑原告之臆測或間接證據（如一般新聞報導、公益團體聲明）並不足以證明個資外洩之來源及途徑，進而無法證明被告之特定行為與原告損害



doi:10.6342/NTU202501770

間具有可預見性或通常性的因果連結。此種嚴格審查標準將有助於法院未來在處理個資外洩案件時，有更為穩健且可預測的標準，避免侵權責任無限擴張。

(三) 個資法與侵權責任關聯之釐清：本案判決另一重要影響在於法院明確釐清個資法第 27 條與民法第 184 條第 2 項間之適用關係。法院清楚界定個資法所規定之安全義務違反，須明確證明被告之特定行為違法，且須有具體條文依據；同時，法院亦強調被告違反此種義務，須與損害發生間存有明確相當因果關係。這一司法態度凸顯法院未來在處理個資法相關案件時，將更嚴謹地要求原告具體指出被告之違法義務內容，而非僅依一般性指控便足以請求賠償。

(四) 法院對間接證據與媒體報導證據力之審慎態度：本案法院明確表示，新聞報導、一般網站聲明或第三方公開資訊，若未能具體指出確切資料來源、資料外洩之具體途徑或被告實際管理、持有個資之事實，則該等證據將無法作為原告勝訴之基礎。此一態度將影響未來個資外洩案件中當事人對間接證據之使用，訴訟策略上需更為嚴謹地蒐證，以具體且直接的證據為主，避免因證據不足而遭法院駁回。

(五) 未來發展之建議

1. 從未來發展角度觀察，本案所凸顯之舉證困難，建議司法實務未來可參考歐盟 GDPR 第 82 條所採行的部分舉證責任轉換或推定過失制度，即在被告明確持有大量個資時，若發生外洩事件，由被告負責舉證排除其過失，以更符合現代風險分配理念。同時，建議未來企業應強化事前的資安措施及資料追蹤機制，司法實務亦可逐步建立相應的判斷標準，降低資料外洩案件中之舉證困難。此外，從立法政策角度，建議立法者檢討現行個資法及侵權責任制度，考慮建立更清晰的法定賠償或懲罰性賠償機制，提供更有效的司法救濟途徑，亦能提升企業履行資安義務的動機。

2. 綜上，本案一二審判決明確界定了舉證責任、相當因果關係以及個資法適用的法律標準，未來不僅能幫助企業明確其法律義務，也將影響受害者在訴訟策略上之舉證要求。此判決亦提供未來法律制度改革的契機，立法與司法實務若朝向更公平有效之救濟與風險控管機制發展，將更符現代社會對個人資料保護的



doi:10.6342/NTU202501770

期望。

## 第七項 威尼斯國際事業股份有限公司個資外洩案

裁判字號：臺灣新竹地方法院 111 年度竹東簡字第 48 號民事判決、臺灣新竹地方法院 112 年度簡上字第 143 號民事判決

一、案件事實

(一) 原告起訴主張：原告主張其於 109 年 12 月 12 日透過被告威尼斯國際事業股份有限公司（下稱威尼斯公司）經營之「威尼斯溫泉露營地」訂房網站輸入手機號碼及信用卡資訊，完成 110 年 1 月 15 日之住宿預訂。該網站係由被告威尼斯公司自行管理後臺，並使用揚京快客行銷公司所提供之虛擬主機空間。109 年 12 月 29 日，原告即接獲冒稱被告威尼斯公司員工來電，訛稱信用卡扣款有誤，並引導其依指示操作 ATM 退款流程，最終遭詐騙 283,115 元。原告進一步指出，其個資僅提供於該訂房網站，且同時期多位顧客亦接獲類似詐騙電話，被告威尼斯公司並曾在官方臉書公告暫停訂房系統與發布警示訊息，足認資料確係自被告威尼斯公司處外洩，與其所受財損間具備相當因果關係。揚京公司後續函文亦揭露被告網站後臺未實施雙重驗證、未遮蔽客戶資訊等資安缺失，顯見被告威尼斯公司未盡個資法第 27 條第 1 項所定「應採取適當安全措施」之義務。另原告亦主張，被告威尼斯公司於 109 年 12 月 28 日即已知悉個資外洩，卻遲至當日晚間或翌日始陸續以簡訊通知客戶，傳送更歷時 5 日才完成，違反個資法第 12 條所規定「應以適當方式通知當事人」之義務。綜上，原告依據個資法第 12 條、第 27 條、第 29 條及民法第 184 條規定，請求被告威尼斯公司賠償其財產損失 283,115 元及訴訟費用。

(二) 被告抗辯：原告並未提出具體證據證明其遭詐騙所使用之個資係由被告威尼斯公司經營之訂房網站洩漏。該網站雖係由被告威尼斯公司管理，但虛擬主機係委由揚京快客行銷公司代管，非由被告威尼斯公司自行維護，且揚京公司並未回報任何資安異常，亦無其他顧客反映資料外洩問題，難以認定資料洩漏源自被告系統；更不能排除原告個人裝置遭駭等其他可能來源。被告威尼斯公司並主張其自 107 年起即使用正版微軟作業系統及內建防火牆，未曾發生入侵事件，客戶資料僅存放於第三方雲端空間，僅透過授權介面查閱訂單資料，未



doi:10.6342/NTU202501770

自行留存個資，且網站運作過程並無異常，已符合個資法第 27 條所要求之合理安全維護標準。另關於個資法第 12 條之通知義務，被告威尼斯公司認為當時僅有個別顧客反映接獲詐騙電話，尚無明確證據證實資料外洩，惟基於善意仍於 109 年 12 月 28 日凌晨即在官網發布警示、報警處理、暫停訂房系統，並陸續發送 1,900 封簡訊通知客戶，已符合法律所稱「適當方式」通知義務。被告威尼斯公司進一步主張，即便假設原告個資係由其網站外洩，原告仍應就詐騙行為與該資料間存在「相當因果關係」負舉證責任；惟本案中詐騙電話號碼與被告威尼斯公司或銀行明顯不符，所稱訂單號碼與實際交易亦不一致，原告應能辨識信用卡退款作業無須透過 ATM 操作，顯見其因個人疏忽而受騙，難以歸責於被告威尼斯公司，且即便法院認定被告威尼斯公司構成違法，仍應依民法第 217 條準用規定，考量原告自身對損害發生具過失而減輕其責任。綜上，請求法院駁回原告全部訴訟請求。

二、法院判決理由分析

(一) 一審判決[86]

1. 關於損害賠償責任之法律構成與個資法適用關係：法院首先指出，個資法之立法目的在於保障個人資料所涉之人格權，並促進合理利用，相關條文包括第 12 條（侵害發生時之通知義務）、第 27 條第 1 項（應採行適當安全措施）及第 29 條第 1 項（損害賠償責任）。其中，個資法第 29 條第 1 項明示非公務機關違反法定義務，致個人資料遭不法利用或侵害者，原則上應負損害賠償責任，僅得以證明無過失為抗辯，故屬一種過失推定責任。法院接續指出，雖個資法與民法在構成要件上不盡相同，但個資法可視為對民法侵權責任之特別規定。然而，無論依民法或個資法，損害賠償之成立仍須具備「損害事實」、「有責行為」與兩者間「相當因果關係」三要件。如無法證明此等要件，則原告即無從主張損害賠償。最高法院亦有相關裁判先例確認此原則，並強調「相當因果關係」係衡量行為與結果間可預測性之重要標準。

[86] 臺灣新竹地方法院 111 年度竹東簡字第 48 號民事判決。



doi:10.6342/NTU202501770

2. 關於被告威尼斯公司洩漏個資事實是否存在之認定：原告主張其於 109 年 12 月 12 日在被告威尼斯公司營運之訂房網站完成訂房後，不久即接獲詐騙集團來電，該等人以能詳述其訂房細節為由騙取其匯款，致其損失 283,115 元。為證其主張，原告提出多項證據，包括訂購資料、電子發票、檢察署之起訴與不起訴處分書、轉帳紀錄與警方案卷，並有被害人證人劉珮琪之證詞佐證。法院進一步調閱新竹地檢署詐欺案案卷，確認被告威尼斯公司之負責人曾供稱曾接獲多名客戶來電反映遭冒用資料進行詐騙，並表示詐騙集團係利用訂房系統中留存之訂金付款紀錄、刷卡資訊等資料進行詐術。同日被告威尼斯公司亦曾於 Facebook 貼文示警，並公告暫時關閉訂房系統以防範個資洩漏。法院認為，綜合上開客觀資料與被告威尼斯公司自陳內容，可認原告訂房資訊確曾由被告威尼斯公司所管理且外洩，且該資訊為詐騙集團實際所使用之資料內容。至於被告威尼斯公司辯稱該資料可能係由詐騙集團入侵原告電腦所取得，並無具體佐證，法院認為不足採信。

3. 關於被告威尼斯公司是否違反個資保護法安全維護與通知義務之認定：法院認定，被告威尼斯公司確曾透過系爭訂房網站取得原告訂房個資，依個資法第 27 條第 1 項，應採取「適當之安全措施」防止該等資料遭竊取、洩漏或滅失，並於發生侵害時，依第 12 條通知當事人。雖被告威尼斯公司主張其已有防火牆、委由廠商管理系統且未接獲異常通報，亦已於 109 年 12 月 28 日凌晨於官網公告提醒詐騙風險，並透過電話與簡訊通知部分客戶，然法院參酌施行細則第 12 條第 2 項對「適當措施」之實質標準，認為被告威尼斯公司僅倚賴廠商系統管理與事後公告，無法證明其事前即已落實合理資訊保護制度，構成安全維護義務之違反。且被告威尼斯公司既知至少已有兩位客戶受害，卻未即時通知包括原告在內之所有潛在受害者，顯未盡通知義務之責任。法院並指出，被告威尼斯公司雖辯稱已報警與通知部分客戶，但仍未全面、即時、具體告知原告，造成原告無法預防進一步損害，應認構成個資法第 12 條與施行細則第 22 條所定之通知義務違反。

4. 關於被告威尼斯公司洩漏資訊與原告財產損害間是否具相當因果關係之判斷：法院於本段重申，損害賠償之構成須有「損害」、「行為」與「相當因果關係」，後者需從事後以客觀方式，依一般經驗法則加以判斷是否通常可由該條件產生



doi:10.6342/NTU202501770

該結果。雖被告威尼斯公司確有違反個資保護義務，致原告個資遭洩，且該資料確為詐騙所用，然法院認為資訊洩漏與詐騙之間仍存在「獨立第三人不法行為」之介入因素。即詐騙之損害究係源於詐騙集團施用詐術與原告錯信操作匯款所致，非個資洩漏本身直接導致損害。就一般情形言，資訊外洩不必然導致財產損害發生，故難認原告損失與被告威尼斯公司洩漏個資之過失間有法律上之相當因果關係。法院並援引最高法院相關判例（如 98 年度台上字第 673 號）支持此見解，強調不得以行為人具過失即當然成立因果關係，須具備客觀條件下之相當性。

5. 原告請求財產損害賠償之主張不成立：綜合上開判斷，法院認為雖被告威尼斯公司確有違反個資法第 12 條與第 27 條第 1 項規定，構成不法外洩行為，亦未即時履行通知義務，然原告所主張之 283,115 元財損係由詐騙集團所施詐術所致，無法確認係由被告威尼斯公司行為直接導致，兩者間欠缺法律上相當因果關係。故依個資法第 29 條及民法第 184 條請求之財產損害賠償請求，應認為不具備要件，原告之請求無理由，應予駁回。

(二) 二審判決[87]

1. 法院認定詐騙集團所使用之個資即來自被告訂房系統，具事實與經驗基礎：法院認為，原告主張於被告威尼斯公司營運之網站訂房並提供手機、信用卡等個資後，即接獲假冒員工之詐騙來電，依指示操作匯款而損失 283,115 元，並提出檢察署不起訴處分書與銀行轉帳紀錄佐證，且被告不爭執此事實，堪認為屬實。再者，另有其他多名客戶亦於同一時期遭同樣手法詐騙，並有證人證述、刑事判決與處分書佐證。此外，自被告於社群平台公告後，留言區亦有十餘名消費者反映接獲類似詐騙電話，內容皆與被告威尼斯公司掌握之訂房資料相符，顯示詐騙集團所持資訊並非來源多元，而係集中源自被告威尼斯公司之系統。雖被告威尼斯公司主張其系統無駭入跡象，且可能是客戶個人設備外洩，但法院認為在無其他合理來源解釋下，依據事實數量、相似性及可得性判斷，

[87] 臺灣新竹地方法院 112 年度簡上字第 143 號民事判決。



doi:10.6342/NTU202501770

該些被害人個資係自被告威尼斯公司之系統外洩最為可採。

2. 法院認定被告威尼斯公司就訂房資料未採取適當安全維護措施，未能舉證排除過失：法院指出，依個資法第 27 條及第 29 條規定，非公務機關若未採取適當資安措施致個資外洩，除能證明無故意或過失外，應負賠償責任。本案中，被告威尼斯公司雖稱已制定內部電腦設備管理辦法、個資保護規則，並由揚京公司設計並代管網站系統，惟法院檢視該等文件內容，發現其多為一般性內部管理規則，無針對客戶個資存取、加密、登入驗證等具體保護機制。且網站系統完成後之日常管理帳號密碼由被告威尼斯公司掌握，實質控制個資者為被告，而非揚京公司。法院亦注意到，事發後系統才補加兩段式登入驗證、遮蔽部分個資，顯見事前保護機制不足。另被告公司規模不小，營收數千萬元，理應有資源建立足夠的保護制度，卻對外洩風險未有有效防範，未能證明無過失，應認對外洩結果負過失責任。

3. 法院認定個資外洩與財損間具備相當因果關係，應負損害賠償責任：法院援引個資法第 29 條及民法第 184 條第 2 項，強調構成損害賠償之三要件為：有損害、有過失或故意行為，以及兩者間之相當因果關係。就本案言，法院指出，原告提供個資予被告威尼斯公司後不久即遭詐騙，詐騙過程中所使用資料即為原告於訂房時所填資料，且詐騙集團係以掌握訂房明細來建立信任，再誘導原告分段匯款。法院認為，若無資料外洩，詐騙即無從精準聯繫與構建話術。加上同時期多位客戶遭同樣詐術得逞，屬可預期風險類型，非偶發事件，故應認外洩行為與財損間具備實質因果與法律上的相當性，為損害發生之不可欠缺條件。原審否定因果關係未及考量風險社會下之高預測性與系統性侵害，認事用法有誤。

4. 法院認定詐騙手法具連貫性，損害非獨立分割事件，應就全部金額認定為外洩所致：法院對於被告威尼斯公司主張僅第一筆「12 元」匯款與個資外洩有關，餘七筆高額匯款屬後續獨立詐騙行為，認為不可採。依原告陳述及轉帳紀錄，原告係在一次通話中，依詐騙集團指示進行多筆所謂「驗證」操作，且初期 12 元退還成功乃為建立信任之手法，後續匯款即連貫發生，非獨立事件。法院並指出，所有匯出款項均係在短時間內連續執行，基於相同詐騙情境、相同資料



doi:10.6342/NTU202501770

來源與心理機制誘導完成，應視為單一詐騙結果。因此，全數金額 283,115 元皆係以個資外洩為基礎所發生之詐騙結果，與被告威尼斯公司未盡資安義務之過失行為具相當因果關係，應就全部金額負賠償責任。

5. 法院認定原告對損害結果有輕忽查證過失，應自負七成責任，被告威尼斯公司負三成賠償責任：法院進一步適用民法第 217 條，就被害人與有過失部分進行判斷。雖然被告威尼斯公司確有過失外洩個資，致使原告遭詐騙，但法院亦指出，當前詐騙手法已屢見不鮮，警政機關與媒體多有宣導，民眾應有所警覺。原告為成年人，於操作匯款前本可查證該來電是否真為店家或銀行所致，或注意到來電顯示不符常理，卻仍未確認即依指示匯出高額款項，對損害之發生具相當助因作用。法院據此認為，雖詐騙源起於個資外洩，但原告未審慎查證，應自負七成過失責任。被告威尼斯公司就餘下三成損害應負賠償責任，折算後應賠金額為 84,935 元，餘額不予支持。原審未認定部分因果關係與過失分擔，改判此部分為適法。

三、判決影響與未來發展之分析

本案原告於威尼斯溫泉露營地網站訂房並輸入個資後遭遇詐騙，損失 283,115 元，遂主張被告威尼斯公司資安疏失致個資外洩並請求損害賠償。被告則否認資安漏洞及因果關係，並主張原告自身輕信詐騙。一審認定被告違反個資法第 27 條（資安義務）及第 12 條（通知義務），但認為詐騙屬第三人獨立行為，與被告威尼斯公司行為間欠缺相當因果關係，駁回原告請求。二審則採較寬鬆之因果推論標準，肯認原告個資確自被告威尼斯公司處外洩，詐騙行為與外洩資料高度相關，足具可預見性，構成相當因果關係。然原告未查證匯款指示，亦有過失，依民法第 217 條準用，酌定其自負七成責任，判被告威尼斯公司賠償 84,935 元。

(一) 加強資安責任標準與個資保護實質審查

1. 本案二審判決的重要突破，在於其對資安保護義務與企業過失認定採取實質而非形式審查的立場。傳統上，法院在類似案件中常以「是否有駭客入侵報告」、「是否接獲異常通報」作為資安過失判斷的主要依據，使得企業若無明確入侵紀錄，往往可否認外洩事實，進而免責。然此種過度依賴形式證據的標準，對於無法掌握技術資訊來源的被害人極不利。



doi:10.6342/NTU202501770

2. 本案中，法院縱使未見明確入侵紀錄，仍綜合「多名受害人訂房資訊之高度一致性」、「詐騙內容與被告網站所掌握資料完全相符」、「被告事後補強資安機制」等事實，合理推論洩漏源頭確為被告威尼斯公司網站系統。此舉不僅符合個資法第 27 條第 1 項對「採取適當安全措施」之立法目的，更符合「實質責任審查」的風向。法院並指出，被告營收規模不小，應具備相對資源採取更高資安標準，惟其未採用雙重驗證、未加密關鍵資料，顯已違反一般社會通念所期待之合理保護義務。

3. 該判決實質上傳達一項警訊：企業不能僅倚賴形式合規文件與外包委託，應對個資控管流程負最終責任。未來法院若普遍採納此種「結果導向」與「風險可預測性」判斷模式，將倒逼企業重視資訊管理內控，強化自主管理與預防性治理能力。

(二) 相當因果關係之實質化與風險社會思維引入

1. 本案二審另一項顯著貢獻，是將「風險社會下的高預測性犯罪」納入相當因果關係的法律評價之中。過往實務上，法院往往認為詐騙行為具有獨立性，資料外洩僅為間接背景因素，因此否定資料提供方與詐騙損害間之法律連結。但在現代網路詐騙場景中，詐騙集團正是仰賴這些經由平台獲取的精準個資，進行具體化、人格化的詐騙操作。倘若無精準資訊佐證，其詐術效果將大打折扣。

2. 本案中，法院明確指出詐騙者係透過原告訂房資料來建立信任，再誘導操作 ATM 匯款，顯示資訊外洩與詐騙有高度工具性連結。而且，同一時期多位消費者接獲類似詐騙電話，均引用被告威尼斯公司網站所載資訊，顯示詐騙內容與外洩來源非巧合，乃系統性結果。此種判斷方式不僅凸顯外洩資料與結果之間的「可預測性」，更重視整體風險結構，將「資料洩漏—第三人不法利用—消費者信任錯置—財損發生」這一鏈條視為法律上可歸責的連續因果鏈。

3. 未來若能廣泛應用此種「風險型因果推論」，可望打破以往對因果關係的高門檻，對受害人而言將大幅改善舉證環境，並促進法院承認數位時代下的高風險結構所產生之實質危害。

(三) 責任比例與消費者自我保護義務之平衡



doi:10.6342/NTU202501770

1. 雖然本案最終由原告部分勝訴，惟法院亦未完全排除其自身在損害發生過程中的過失。二審法院適用民法第 217 條，指出詐騙手法已被社會廣泛揭露與宣導，民眾應具備基本防詐警覺。原告在未確認對方身分即依指示匯款高額金額，屬可避免風險而未避免者，應自負部分責任。法院據此認定原告對結果應負七成責任，被告僅負三成。

2. 此一責任比例調整機制兼顧了二個價值：其一，避免企業完全免責，有助於督促其改善資訊保護與內控機制；其二，提醒消費者於資訊使用過程中仍須保持基本警覺義務，避免資訊社會責任全然單邊化。未來若能形成穩定見解，亦有助於促成「資訊提供者—資訊使用者」間之風險共同管理與防詐聯防模式。

(四) 結論與制度反思

1. 本案所揭示之法律爭點與實務突破，對於我國個資損害賠償制度建構具重大啟示意義。首先，在實體法層面，法院強化個資法第 27 條安全維護義務之可執行性，並對第 29 條損害賠償責任條款採取較具啟發性的詮釋方式，使法律保護效果更具實質意義。

2. 其次，在程序法面向，法院展現對間接證據與集體性事證（如多名受害人、相似詐騙內容等）之整合運用能力，不再機械要求被害人提出「資料從何處外洩」之直接證據，而是透過推定、比對、歸納，建構法律上的外洩來源與因果推論。此一作法降低了被害人舉證難度，對實務審理將產生積極導向。

3. 制度上，政府未來應朝以下幾個面向進行強化：一是導入「資料洩漏推定責任」條款，仿效 GDPR 第 82 條責任推定邏輯，要求明確掌握資料之業者負反證義務；二是建立資料流向記錄與技術溯源義務，透過技術工具（如資料指紋、存取紀錄等）輔助法院審理；三是明文化個資外洩後通知義務與內容要件，避免企業簡單公告即行免責。

## 第八項 迪卡儂個資外洩案

裁判字號：臺灣臺中地方法院 111 年度訴字第 2708 號民事判決、臺灣高等法院臺中分院 112 年度上易字第 208 號民事判決



doi:10.6342/NTU202501770

一、案件事實

(一) 原告起訴主張：其於 108 年 3 月間透過被告迪卡儂股份有限公司（下稱迪卡儂公司）經營之線上購物平台進行消費，並為使用相關服務，於平台上填寫姓名、生日、手機號碼、地址、電子郵件等個人資料，成為會員。惟被告迪卡儂公司未依個資法第 27 條第 1 項及第 12 條之規定，採取適當安全措施保護其個人資料，導致資料外洩事件發生。該外洩情形於 111 年 5 月 2 日經第三人向媒體揭露後，被告迪卡儂公司並未積極查明事實及即時通知可能受影響之會員，反而消極否認資料外洩。其後，原告於同年 5 月 18 日接獲詐騙電話，詐騙集團佯稱系統被駭、原告資料遭冒用註冊為高級會員，將有低消扣款風險，如欲解除需操作網銀。原告信以為真，依指示分次匯款，合計損失 571,573 元，並因此遭受精神痛苦。原告依個資法第 29 條第 1 項請求被告迪卡儂公司賠償財產上損害 571,573 元，另依同條第 2 項準用第 28 條第 2 項，主張非財產上損害賠償 20,000 元，共計請求 591,573 元。

(二) 被告迪卡儂公司抗辯：原告之個人資料非從被告之資料庫洩漏，而是詐騙集團透過其他管道取得。被告迪卡儂公司有採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏，並未違反個資法第 27 條規定。被告迪卡儂公司早於原告遭到詐騙之前，即於 111 年 4 月 26 日在官網利用彈出視窗、LINE 推播訊息及在臉書粉絲頁發佈反詐騙公告，提醒消費者預防詐騙，並於翌日向會員發出反詐騙提醒簡訊及電子郵件，並未違反個資法第 12 條規定。原告遭受詐騙，係因詐騙份子積極實施詐騙行為所致，與原告個人資料遭到不法蒐集不具相當因果關係。且原告匯款時間前後差異時間達 7 個小時，不合常理。

二、法院判決理由

(一) 一審判決[88]

1. 法院對原告個人資料為被告保有且外洩之認定：法院首先認定原告於被告迪卡

[88] 臺灣臺中地方法院 111 年度訴字第 2708 號民事判決



doi:10.6342/NTU202501770

儂公司之線上購物平台購物時，確已提供姓名、地址、手機、電郵等個人資料，並有歷次訂單紀錄及個資紀錄為證，被告迪卡儂公司亦不爭執原告曾於其平台消費。再者，根據刑事警察局於 111 年間之通報，被告名義之詐騙事件在短時間內數量暴增，並多次被公告為「高風險賣場」，另其臉書公告下亦有多名消費者反映遭遇與原告相似之詐騙手法，顯見詐騙集團所掌握之資訊包括消費明細及聯絡資料，足認係從被告迪卡儂公司端洩漏。法院綜合客觀證據，認定原告個資係由被告迪卡儂公司所保有並洩漏，否定被告迪卡儂公司主張資料係自他途外洩之抗辯。

2. 法院對被告迪卡儂公司未採取適當資安措施之認定：檢視被告迪卡儂公司所提出資安措施，包括伺服器安全群組設定、內部管理文件、對經濟部回函及與第三方廠商間之契約條款，發現其中多項政策至原告受騙時仍處於「擬訂中」狀態，顯示資安規劃尚未實質落實。且被告迪卡儂公司提出多數措施係發生外洩事件後始行補強，難以證明其事前已採取適當保護機制。加以所稱與廠商之合約約定，僅能反映雙方法律義務安排，並非具體安全技術措施，難認足以防止個資洩漏。法院因此認定，被告迪卡儂公司並未依個資法第 27 條第 1 項規定，於原告遭詐前即採行足夠安全措施。

3. 法院對相當因果關係之判斷：法院於因果關係部分，引用最高法院 83 年度台上字第 2261 號判決所示之「相當因果關係」標準，指出被告迪卡儂公司怠於資安維護，致其所保有之個資（包括購物紀錄）遭詐騙集團不法取得，並用以對原告進行有目的性之詐騙，最終造成具體財損。此等行為係該怠惰行為按一般情形所可生之結果，故應認兩者間具相當因果關係。法院據此駁斥被告所稱「純屬詐騙集團行為，與己無關」之抗辯。

4. 法院對個資法第 12 條通知義務之解釋：法院於通知義務部分指出，儘管原告聲稱未收到電子郵件與簡訊通知，然被告迪卡儂公司已於官網與社群媒體公告警示資訊，並附有發送紀錄佐證。考量被告迪卡儂公司為大型電商企業，會員眾多，依個資法第 12 條之立法理由，可採公告方式為適當通知手段。故法院認定，被告迪卡儂公司雖未個別告知原告，但其公告已足符合法條要求，並未違反通知義務，原告就此請求無理由。



doi:10.6342/NTU202501770

5. 法院對原告財產損害與精神損害之認定：法院認定，原告因個資外洩而遭詐騙，實際損失匯款金額 571,573 元，屬於財產上損害，另因隱私權侵害與事件衝擊，亦足生精神痛苦，得請求非財產上損害賠償。法院斟酌原告社經地位、職業背景（碩士學歷、律師職業）、財務狀況、加害人性質及被告企業規模等因素，認原告請求非財產損害賠償 2 萬元為適當，予以全額認可。

6. 法院對原告過失責任之評價與過失比例劃分：雖法院認定原告所受損害與被告洩漏個資具因果關係，惟於責任比例部分，法院考量原告本身具備高度社會知識與法律專業，且為律師，應對詐騙風險具有合理警覺，卻仍於長達 7 小時內依照詐騙指示陸續匯款。加以當時社會對於「解除分期付款詐騙」已有明確警示，原告應有合理預見義務，卻未積極查證。故法院認原告對損害應負 90%之過失責任，僅認被告需負 10%，即應賠償金額為 59,157 元。

7. 綜合上述，法院認原告請求部分有理由，部分無理由，依個資法第 29 條第 1 項及第 2 項準用第 28 條第 2 項，判令被告迪卡儂公司應賠償原告 59,157 元及自 111 年 7 月 8 日起至清償日止按年息 5%之利息。

(二) 二審判決[89]

1. 被告迪卡儂公司未盡個資保護義務，違反個資法第 27 條，構成過失：法院確認，依個資法第 27 條第 1 項、第 29 條第 1 項及第 2 項之規定，非公務機關保有個人資料而未採取適當安全措施，致個資外洩，原則上推定其具有故意或過失。除非能證明「無過失」，否則須負損害賠償責任。法院指出，被告迪卡儂公司雖提出伺服器設定、防火牆、資安檢測等資料作為抗辯，然其資安內控政策多尚在「擬訂中」，且多數改進措施係於個資外洩後始行實施，難以證明事發前即已妥適防範。此外，與物流業者間之 SFTP 設定、安全監控及資料加密措施亦明顯不足，資訊傳輸風險高。法院因此認定，被告迪卡儂公司未盡個資安全維護義務，構成過失。

2. 法院認定資料來源係被告迪卡儂公司，個資確有外洩：法院參考刑事警察局公

[89] 臺灣高等法院臺中分院 112 年度上易字第 208 號民事判決。



doi:10.6342/NTU202501770

告，自 111 年 5 月起迪卡儂客戶遭詐事件爆量，通報件數暴增超過 500 件，並曾被連續公告為高風險賣場。再者，臉書粉專大量客戶留言指出詐騙集團可準確說出其購買明細與金額等個資細節，且被告迪卡儂公司並不否認此等留言內容。法院認為，詐騙集團所使用資訊高度細緻，顯屬交易平台內部資料，不可能從公開管道取得，足證資料即係從被告迪卡儂公司或其協力廠商外洩，非如被告迪卡儂公司所稱係「第三方途徑」所致。

3. 雖違反個資保護義務，惟與詐騙金錢損害間不具相當因果關係：雖法院已確認被告迪卡儂公司對個資外洩確有過失，並違反個資法第 27 條，惟於相當因果關係判斷上，法院採嚴格審查標準。法院認為，原告所受 57 萬餘元之財產損失，係詐騙集團實施詐術所致，屬第三人積極犯罪行為，與被告迪卡儂公司之過失間不具「一般情形下可預見並足生此結果」之關聯。換言之，即便被告迪卡儂公司未善盡資安義務，但並不當然導致原告遭詐騙並財損。法院據此否定兩者間之「相當因果關係」，故就財損部分請求不予准許。

4. 就非財產損害部分之肯認與裁量：法院肯認被告迪卡儂公司未善盡資訊安全義務，已侵害原告之隱私權與個資自主權，構成不法侵害，應負非財產上損害賠償責任。法院進一步指出，原告因個資外洩而飽受精神困擾，並須耗費心力進行申訴與防範，屬個資法第 28 條第 2 項之損害情形。法院依被告企業規模、原告社經地位及侵害程度等斟酌，認賠償金額以 2 萬元為妥當。

5. 就個資法第 12 條通知義務部分，被告迪卡儂公司未違反法定義務：對於原告主張被告迪卡儂公司未即時個別通知其個資遭洩漏一節，法院依個資法第 12 條之立法理由認為，於會員人數眾多情形下，非公務機關得以「公告」替代個別通知。被告迪卡儂公司已於官網、臉書發布反詐騙公告，並嘗試發送簡訊與電郵（雖原告稱未收到），應認已履行通知義務，未違反第 12 條規定，故原告依此項主張請求賠償無據。

6. 法院綜合認定，被告迪卡儂公司違反個資法第 27 條規定，確對原告個資保護疏失而構成過失，並致個資外洩，侵害隱私權與個資自主權。惟該違法行為與詐騙集團實施之詐欺犯行並不具「相當因果關係」，原告對金錢損失之請求無據，僅得請求 2 萬元非財產損害。法院因此廢棄原審就全部賠償範圍之認定，



doi:10.6342/NTU202501770

改判僅准非財產損害部分，其餘駁回。

三、判決影響與未來發展之分析

被告迪卡儂個資外洩案歷經一、二審審理，法院均肯認企業未善盡個資保護義務，構成個資法第 27 條所禁止之違法行為，惟在損害賠償部分，一審採取過失與因果關係並存且部分減責的立場，判准企業賠償部分財損與非財損；而二審則雖維持違法與過失之肯認，但否定財產損害與企業行為之間的相當因果關係，僅准非財產損害賠償請求。此一判決思維反映我國法院在個資外洩與詐騙損害糾紛中，對侵權責任構成要件的逐步嚴謹化，同時也對企業在資訊安全義務的落實及責任預測帶來重要啟示。

(一) 法院實務對「過失推定」的適用標準日益具體化

依據個資法第 29 條第 1 項但書，若非公務機關所保有個資遭洩漏，則推定其具有故意或過失，唯有舉證證明無過失者，始得免除賠償責任。本案中，法院即援引該條文與第 27 條之安全維護義務，指出企業若未能事先建立具體而可驗證之資安制度，即構成過失行為。尤其值得注意的是，法院明確指出僅提出「資安內控政策擬訂中」或「事發後改善措施」者，無法構成已盡安全維護義務的證據，顯示法院不僅審查形式規範是否存在，更重視事前風險防範機制是否已實際落實。此外，對於與第三方（如物流或 IT 廠商）間的合約關係，法院亦採取實質審查標準，強調資料控制責任不可輕易透過契約外包加以切割。此一實務趨勢對企業而言極具警示意義。未來若欲主張免責，應建立包括資料加密、權限控管、傳輸保護、事後通報等多層次防護架構，並應對所有委外服務建立可稽核之資訊安全責任鏈條，以備於訴訟中提出可佐證其已盡義務的資料。

(二)「相當因果關係」之判斷標準朝向保守立場發展

本案二審法院縱使認定企業已違反個資法規定，但於是否對原告遭詐之財產損害負責部分，則轉向採用嚴格的相當因果關係標準，認為詐騙行為為第三人所為，具主觀惡意、詐術運作、乃至與原告認知行為高度連結，難認為企業洩漏個資即為導致財損之「通常可預見結果」。此種因果關係否定，實際上大幅限縮企業在個資外洩事件中對財損部分的損害賠償責任。除非消費者能舉證詐騙內容與洩漏資料高度對應、企業資安漏洞具持續性且可預見風險，否則在法院審理下，難以證



doi:10.6342/NTU202501770

立法律上之連結性。值得注意的是，一審法院採「風險實現理論」，認為企業未妥善管理個資，已實質促成詐騙發生機會，而該風險已於本案中具體實現，故應負部分責任。但二審則明確與該見解切割，重申「詐騙為獨立中斷因素」，凸顯法院見解尚未一致。未來倘欲建立更明確與合理之因果判準，仍有賴最高法院或立法機關之指引與制度補強。

(三) 精神損害認定成為個資外洩案中實際可得賠償之重心

儘管本案二審法院否定原告對財產損失部分之請求，但仍明確肯認原告個資被洩所造成之隱私侵害、精神壓力與申訴困擾，構成非財產上損害，准予賠償 2 萬元。此一處理方式符合近年實務傾向，即當被害人未能就財損與企業行為建構法律上因果關係時，仍可基於人格權侵害主張非財產損害賠償。然而，法院對精神損害之認定與金額核定，亦日益趨於「節制與合理性」原則，並考量被害人社經背景、企業規模與事後回應態度等要素。此亦意味，非財產損害賠償不再具有懲罰性或標準化性質，未來消費者仍須具體主張自身因個資外洩而產生生活干擾或精神壓力的具體情節，方能獲法院支持。

(四) 對第 12 條通知義務之實務界定有助企業降低合規風險

在個資外洩後之應變義務部分，法院對個資法第 12 條「應即時通知當事人」之規範，採取彈性解釋，認為在會員數量龐大情況下，企業得以公告方式代替個別通知，並肯認被告透過官網、社群平台公告與簡訊發送等作法已符合法律要求。此一解釋不僅考量實務操作彈性，亦反映法院認知數位環境下之「適當通知方式」應兼顧可及性與資訊傳播效率。對企業而言，此一見解提供實務參考方向，未來如能證明曾採多元渠道廣泛通知，且方式具實質可得性，即可作為履行第 12 條義務之證明。

(五) 綜合以上觀察，本案對我國個資保護訴訟實務產生三大關鍵影響。首先，法院逐步建構出具體的資安義務審查標準，促使企業應於事前積極落實內控制度；其次，在損害賠償責任判斷上，因果關係成為勝敗關鍵，代表消費者需更加強化證據鏈結才能請求財損；第三，精神損害成為個資案件實務中較可能獲賠的範疇，但其成立亦日趨嚴格，非純形式主張即能成立。在制度面上，未來可思考是否藉由修法或行政命令形式，進一步明定「過失推定之舉證準則」與「可



doi:10.6342/NTU202501770

推定因果關係情形」，以及對精神損害金額設立參考級距，藉以提升個資保護法的適用明確性與實踐效力。於數位經濟與詐騙手段不斷演變的時代背景下，本案所揭示的裁判標準，將成為企業風險控管與司法責任分配的重要基石。

## 第九項 和雲行動服務股份有限公司 iRent 個資外洩案

裁判字號：臺灣臺北地方法院 112 年度訴字第 3711 號民事判決、臺灣高等法院 113 年度上易字第 471 號民事判決

一、案件事實

(一) 原告起訴主張：原告主張，其因承租被告和雲行動服務股份有限公司（下稱 iRent 公司）所營運之「iRent」汽機車服務，依契約要求提供姓名、手機號碼、電子郵件、住址、駕照照片與信用卡資料等個人資料（以下簡稱「系爭個資」）。惟於 112 年 1 月 31 日，外媒 Tech Crunch 報導揭露，被告 iRent 公司關係企業之雲端伺服器發生資料外洩事件，致原告等 iRent 用戶個資暴露於可供任意存取之網路環境，北市監理所經查認定事故肇因為暫存資料庫未設防護機制，且被告 iRent 公司並未依個資法規定制定個資安全維護計畫，已明確違反第 27 條第 1 項、第 2 項規定，遂對被告處以罰鍰 20 萬元。原告據此提出損害賠償請求，主張第一，依個資法第 29 條規定，被告 iRent 公司既已承認系爭資料庫存有防護性缺口，且於接獲通報後即能於 1 小時內修補，足以證明其先前並未採行當前科技水準下可行之適當安全措施，應就違反安全維護義務所致之個資外洩，負損害賠償責任，並得請求每人最高 2 萬元之非財產損害賠償；第二，依民法第 227 條及第 227 條之 1 規定，雖個資保護非屬契約主要給付內容，然基於附隨義務與完整履約原則，被告 iRent 公司有義務善盡資料安全管理注意義務，其遲至外部通報始知資料庫缺陷，構成契約不完全給付；第三，依民法第 184 條前段及第 2 項規定，被告 iRent 公司對 iRent 系統資料具控制權，對於系爭個資之保管應負積極作為義務，然其未妥善防範資料庫遭外部連線存取，已構成不作為侵權行為；第四，原告援引民事訴訟法第 278 條第 1 項及個資法第 28 條第 3 項，主張主管機關既已作成行政處分認定違法並課以罰鍰，應推定被告 iRent 公司已有過失且原告個資確實洩漏，原告無須再負完全舉證責任。綜上，原告請求法院命被告 iRent 公司就各原告之個資外洩致隱私



doi:10.6342/NTU202501770

權受侵害之事實，分別給付每人 2 萬元，並自起訴狀繕本送達翌日起至清償日止按年息 5%計算之利息。

(二) 被告 iRent 公司抗辯：被告 iRent 公司對上訴人主張其違反個資法第 27 條第 1 項、第 2 項規定、致系爭個資外洩一節，提出明確抗辯，認為依民事訴訟法第 277 條規定，原告應就其主張之有利事實負舉證責任，應自行證明個資確已遭洩漏及損害發生。被告 iRent 公司主張，其於 112 年 1 月 28 日晚間首次接獲資安通報後，立即檢查系統並確認資料庫並未遭第三人入侵，並於第一時間內完成封鎖外部連線，防止進一步風險擴大。嗣後基於風險控管與告知義務，分別於 112 年 2 月 1 日及 2 月 4 日發布聲明稿一、二，僅說明可能存在外洩風險，並提醒用戶提防詐騙，並未承認實際外洩情事。交通部公路局於 112 年 2 月 4 日完成之資安稽核報告亦未載明有 iRent 用戶個資遭不法蒐集、處理或利用。為進一步釐清資安事件，被告 iRent 公司另委託果核數位與精誠資訊兩家資安公司進行檢測，結果顯示主機系統並無資安漏洞，足證 iRent APP 資料未曾外洩。至於交通部於 112 年 2 月 8 日就本案曾裁罰被上訴人 20 萬元，被告 iRent 公司已提起訴願，交通部亦於同年 10 月 5 日自行撤銷該處分，顯示行政機關對其是否違法仍有保留，該處分並不足以作為原告損害賠償請求之依據。此外，原告所援引之 110 年 8 月 30 日 iRent 臉書貼文與留言內容，與本件系爭資料庫資安事件並無直接關聯，為屬不同時點與情境之獨立事件，無法證明被告 iRent 公司當時未採取適當安全措施或因此致個資外洩。綜上，原告未能證明其個資確曾外洩或遭不法利用，亦未舉證具體損害或隱私侵害事實，其損害賠償請求既無事實基礎，應予駁回。

二、法院判決理由分析

(一) 一審判決[90]

1. 舉證責任與損害賠償構成要件的法律適用基礎：本案法院首先援引民事訴訟法第 277 條明文規定，當事人對於主張有利於己之事實，應負舉證之責。進一

[90] 臺灣臺北地方法院 112 年度訴字第 3711 號民事判決。



doi:10.6342/NTU202501770

步依據個資法第 2 條第 1 款、第 28 條第 1 項、第 2 項及第 29 條等規定，法院指出，原告若主張個資損害賠償，須具備三項構成要件：其一，個人資料確曾遭不法蒐集、處理或利用；其二，當事人因此權益受有侵害；其三，加害行為與損害間具有相當因果關係。雖然個資法已採「過失推定」及「舉證責任倒置」原則，惟法院明確強調，倘若原告尚未完成對於「不法處理行為」之初步證明，則無從啟動責任歸屬之推定機制。

2. 原告未舉證有個資外洩事實：就原告是否完成對於不法行為之舉證，法院首先肯認，原告確曾於 iRent 系統內輸入其姓名、聯絡方式、駕照照片與信用卡等資訊，並於事件發生後獲得被告所發出之補償性聲明與折抵券等回應措施。然關鍵爭點在於是否確實發生資料外洩。法院認為，即便 TechCrunch 報導指稱系爭資料庫未設密碼保護，任一知悉 IP 位址者皆可進入，顯示資料處於高風險狀態，但除該名資安研究員 Sen 外，尚無證據顯示第三人曾實際下載、蒐集或處理原告等人資料。加以資料庫於一小時內即被下線，顯見被告 iRent 公司已迅速封堵漏洞。故法院認定，即使存在風險環境，仍不足以推定原告資料實際遭不法處理。

3. 法院對原告輔助證據之證明力評價：針對原告所提出之補強證據，法院逐一予以檢視並駁斥。首先，對於被告發布之「系爭聲明一、二」，法院指出其語詞多以「可能」、「風險」、「倘若」等措辭呈現，屬預防性揭露，未構成個資已外洩之承認。其次，針對北市監理所之行政處分與調查報告，法院認為僅指出資安保護上存在漏洞與計畫缺失，並未具體證明原告個資已被他人蒐集或利用。至於原告引用之社群留言與詐騙電話紀錄，法院以留言者無具體身分、內容無法查證及與案件無直接關聯為由，否定其證據能力與連結性，認為尚不足以支撐個資遭不法處理之主張。

4. 駁回契約與侵權損害賠償之理由：針對原告進一步援引民法第 227 條與第 184 條所主張之契約附隨義務不履行與不作為侵權行為，法院認為該等請求權基礎，仍須先建立「原告個資遭外洩」之客觀事實基礎。然原告既未能證明其資料已實際遭第三人存取、使用或導致權益侵害，自屬欠缺結果要件及因果關係之證明。即便被告 iRent 公司於資安維護上可能存在瑕疵，惟僅因未預防風險



doi:10.6342/NTU202501770

尚不足以成立損害賠償之法定要件。

5. 法院於綜合審酌全案證據與雙方主張後，明確指出原告對於個資遭不法處理一節未能完成舉證，依個資法第 29 條、民法第 227 條及第 184 條所生之損害賠償請求均無理由。

(二) 二審判決[91]

1. 法院確認個資法第 29 條雖設有舉證責任倒置及過失推定制度，惟此制度之適用以「已發生個資不法蒐集、處理、利用或洩漏」為前提。換言之，原告須先證明其個資確曾遭受不法處理，方得進一步推定被告之過失。本案法院據此認定，上訴人未能完成核心構成要件之事實舉證，無從進入責任歸屬之評價。

2. 其次，就原告提出之證據是否足以認定資料洩漏，法院逐一加以檢視。關於台北市監理所之調查函及交通部曾就資料外洩裁罰被告之處分，法院指出，該行政處分已遭撤銷，且調查內容亦未查明特定消費者之個資確遭外洩，故其證明效力有限。此外，交通部委外資安稽核結果亦明確指出並未發現個資外洩事實，反而證實被告已採行適當資安控管措施。

3. 再者，關於媒體報導所稱安全研究員於雲端資料庫中發現未加密之 iRent 用戶資料，法院認為，報導雖揭示存取風險，但僅能證明系統存在漏洞，尚不足以推論原告個資確已外洩。報導中僅一名研究員曾接觸資料，且被告 iRent 公司於通報後一小時內即封鎖資料庫外部連線，無法認定有其他第三人取用資料之事實存在。

4. 關於被告 iRent 公司所發布之聲明稿，法院認為，其文字多採「可能」、「風險」、「預防性補償」等表述，僅屬於風險揭露與消費者告知義務之履行，並未構成對資料外洩事實之自白。原告據此聲明推論個資已外洩，法院認為解釋失當。

5. 此外，原告另提出四名用戶遭遇可疑電話或信用卡盜刷、以及社群留言反映疑似遭詐事件等補強資料。法院認為，上開資料來源無法確證為 iRent 系統，亦

[91] 臺灣高等法院 113 年度上易字第 471 號民事判決。



doi:10.6342/NTU202501770

無具體可驗證之資料外洩路徑，與本案系爭資安事件間缺乏直接因果關聯性。即使原告確曾遭遇詐騙事件，亦未能證明該行為與本案資料庫風險具關聯性。

6. 就原告援引民法第 227 條、第 227 條之 1 及第 184 條主張契約附隨義務與不作為侵權之部分，法院認為，該等法律責任皆須以原告個資確遭洩漏為前提，原告既未能證明不法處理或損害事實，自無從成立給付不完全或侵權責任之評價空間。綜合而論，法院判定原告未能舉證證明系爭個資曾遭不法處理，亦無證據證明個資洩漏與具體損害間存在相當因果關係，故依個資法第 29 條、民法第 184 條、第 227 條等規定提起之損害賠償請求均應駁回。

三、判決影響與未來發展之分析

本件 iRent 資安事件所衍生之損害賠償訴訟，歷經一、二審皆以駁回原告請求作結，法院的主要理由聚焦於原告未能完成對個資實際遭不法處理之舉證，無法引發個資法第 29 條之過失推定機制，且亦未證明其財產損害與該資安事件具「相當因果關係」。此案成為國內個資保護訴訟中極具代表性的裁判例，其影響與啟示可從下列幾個層面加以說明：

(一) 舉證責任分配原則之實務限縮：從風險揭露到實害證明

個資法第 29 條設有舉證責任倒置與過失推定制度，理應在個資確有遭外洩、不法處理等初步事實成立時，反轉由企業證明其已盡安全維護義務。然而，本案法院卻反覆強調：「推定前提」仍需由原告先行證明其個資確已遭第三人不法蒐集、處理或利用，始得啟動過失推定。換言之，法院對原告之舉證門檻設定頗高，即便存在資安漏洞、媒體報導揭露風險、企業發出預防性補償聲明，仍不足以構成「已發生個資不法處理行為」之認定。此舉實質上限縮了個資法賦予消費者的訴訟保障，亦提高受害人在訴訟中須提出的證據難度。未來在無強制調查權或公開揭露機制之情況下，個別消費者若要證明其資料確實外洩並遭不法利用，將極度困難。此勢必影響個資法訴訟之可行性，也顯示現行制度下，法院對舉證門檻與證據能力之解釋，已轉趨保守與形式化。

(二) 法院對風險事實與實際外洩之區分強化了企業防禦邏輯

在法院審理中，儘管原告引用資安報導指出系爭資料庫未設密碼，可能開放予



doi:10.6342/NTU202501770

任意第三人存取，且企業也曾發布「資料風險通知」與補償機制，法院仍強調，風險存在與資料實際外洩乃兩回事。法官進一步區分「潛在漏洞」與「確定外洩」之法律評價意涵，認為若無證明第三人曾實際接觸、蒐集或處理該筆個資，即難以構成違法處理事實，從而無從主張民事損害賠償。此一判斷結果強化了企業防禦主張，即只要沒有外部攻擊紀錄、未出現確切外洩個案，便能避開民事責任的歸屬。對企業而言，此或許有助於界定責任邊界，降低不確定訴訟風險；但對受害消費者而言，則可能造成「除非詐騙成功否則難以求償」的窘境。若法院不承認潛在風險或事後補償行為的法律推定意義，則個資法第 29 條的實質保障效果將大打折扣。

(三) 相當因果關係判準趨嚴：拒絕基於「風險預見性」主張企業連帶責任

本案另一個關鍵爭點在於：即便企業資安系統有缺失、確實產生資安風險，是否就應對詐騙造成之財損負責？法院明確指出，即便原告確實遭遇詐騙並損失金額，亦無證據證明詐騙者所使用資料即來自系爭資料庫，且該詐騙行為多為第三人主觀惡意之詐術所致，無法合理推定為企業行為「通常可預見之損害結果」。此與近年主張「風險實現理論」的判決（如威尼斯露營案、王品案）採取不同見解，後者認為若資料系統外洩導致詐騙集團得以執行針對性誘導，即可視為企業違法行為所致風險已實現，具備相當因果關係。而本案法院則回歸傳統「條件理論＋社會經驗」的因果關係判斷模式，對企業責任採較為保守態度。此一分歧反映我國對「個資外洩與詐騙損害」之因果鏈結，尚無統一見解。若未來高等法院或最高法院能進一步統整相關案例，釐清該等風險是否屬可預見之行為結果，將有助於提升司法穩定性與預測可能性。

(四) 補強證據的證明力爭議：社群留言與用戶回饋是否可納為事實推認依據？

本案亦涉及一項重要實務問題，即法院對「社群證據」與「群體反映」之證明力評價趨於保守。原告雖提供多位用戶留言、可疑來電紀錄、信用卡盜刷回報等資料，法院卻以「內容無法查證」、「與系爭平台無直接連結」為由，否定其證明力。此一態度顯示法院對於來自網路、社群、消費者平台等非正式紀錄之證據能力，仍抱持高度懷疑。然於數位社會中，許多資安事件與詐騙手法往往可由消費者經驗交叉印證，其資訊價值不可忽視。未來若能由行政機關或第三方機構建立事件登錄與彙整機制，或立法將群體證據納入法律推定依據，將有助於彌補個案舉證之困難與



doi:10.6342/NTU202501770

司法資源之限制。

(五) 對契約附隨義務與不作為侵權責任的連動性否定

本案亦否定原告另以民法第 227 條與第 184 條主張之契約不履行或不作為侵權責任。法院認為，無論基於契約附隨義務或一般侵權行為責任，皆須以「資料確實遭洩漏」為構成前提，原告未能證明個資實際被處理，自無從進一步主張契約不完全給付或不法行為成立。此結果顯示法院在個資法與傳統民法責任競合適用時，採取「外洩事實」為唯一切入點，實質上亦限縮了契約相對人針對資安義務未履行之請求空間。未來在平台經濟或數位服務契約中，若希望建構較有力之保護機制，應思考在契約條款中預先約定資安標準與違約責任，以強化求償基礎。

總結而言，本案判決反映我國法院於個資保護訴訟中，對責任認定標準、因果關係判斷與證據評價皆趨於謹慎與形式性，對原告而言舉證負擔沉重，實際救濟門檻高。未來若欲提升個資法第 29 條保障實效，應從制度設計與實務操作兩面加以補強，包括：明確推定條件之立法、建立群體舉證資料平台、推廣預設違約條款於契約中揭示資訊安全義務等，方能實現資訊社會中對個人隱私之有效保護。

## 第十項 神腦國際企業有限公司個資外洩案

裁判字號：臺灣臺北地方法院 112 年度訴字第 2854 號民事判決

一、案件事實

(一) 原告起訴主張：原告於 111 年 9 月 5 日深夜，透過神腦國際企業股份有限公司（下稱神腦公司）經營之「神腦生活」網站平台（下稱系爭平台）下單購買產品，並輸入包括姓名、手機號碼、收件地址及信用卡資訊等個人資料完成付款。原告稱，神腦公司為取得經營利益，留存消費者個人資料，惟卻未採取適當資訊安全維護措施，導致個人資料外洩。原告於同年 10 月 20 日接獲詐騙集團成員冒充神腦公司或台北富邦銀行人員來電，並以其在系爭平台之實際交易資訊為由，誘使原告依指示轉帳，致使原告遭詐騙 699,515 元（下稱「系爭款項」）。原告於 10 月 21 日報案後，警方查獲該詐欺集團，並發現被告李文正參與詐騙行為，擔任取款車手，實際提領該款項 449,966 元，轉交予詐團其他成員。原告認為，李文正作為詐欺行為人或其幫助犯，依民法第 184 條應負



doi:10.6342/NTU202501770

損害賠償責任；即便不認為其構成侵權行為，仍因其無法律上原因取得原告款項，應依民法第 179 條返還不當得利。此外，原告主張系爭交易資訊僅存於神腦公司系統，且神腦平台曾被內政部警政署列為「高風險賣場」，可見神腦公司未採取適當安全措施致資訊外洩，導致原告個資遭詐團蒐集利用。原告據此主張，神腦公司及其負責人林榮賜應依個資法第 29 條第 1 項、第 2 項準用第 28 條第 2、3 項，或民法第 184 條、第 195 條第 1 項等規定，連帶賠償財產損失 69 萬 9,515 元及非財產上損害 2 萬元。原告並進一步認為，神腦公司、林榮賜及李文正三人，係基於各別法律原因而負擔目的相同之金錢給付義務，應屬不真正連帶債務，倘一人給付，其餘債務人即於該範圍內免責。原告遂提起本訴，請求法院判令：李文正應給付原告 69 萬 9,515 元及法定利息。神腦公司與林榮賜應連帶給付原告 71 萬 9,515 元及利息。

(二) 被告神腦公司抗辯

1. 資料來源與外洩事實並未證實，原告應負舉證責任：原告之系爭交易發生於 111 年 9 月 5 日，遭詐騙時間則為同年 10 月 20 日，兩者相距逾一個半月。根據內政部警政署 165 反詐騙專線於 9 月 5 日至 11 日公布之高風險賣場名單，並無被告神腦公司在列。故依一般經驗法則推論，詐騙集團所使用之原告個人資料未必來自系爭平台。原告若主張其個人資料係由神腦平台洩漏，應自負舉證責任，然其未提出具體證據。

2. 可能資料外洩之其他來源未經排除：即便承認資料確有外洩之可能，該等資料亦可能來自被告神腦公司合作之物流業者、其他第三方合作廠商，或因原告自身設備資安不足（如個人電腦遭駭）所致，甚至亦有可能為第三人非法入侵神腦公司資訊系統所為。原告未能排除上述可能性，自難認其所受之損害與被告神腦公司有直接因果關係。

3. 被告已採行當時可期待之資安措施，並無違反個資法第 27 條：被告神腦公司所採行之資訊保護措施已符合當時之技術水準與實務慣行，對所蒐集之個人資料已盡合理注意義務，未有違反個資法第 27 條第 1 項所規定之「避免資料遭不法蒐集、處理、利用或洩漏」義務。

4. 詐騙集團故意犯罪行為中斷因果關係：被告神腦公司進一步指出，即使資料外



doi:10.6342/NTU202501770

洩事實成立，然真正導致原告財產損失者，係詐騙集團之主觀故意詐術行為。該等行為之積極性與獨立性，已中斷即便存在之個資外洩結果與財產損害之相當因果關係。被告神腦公司並無法定或契約上義務防止第三人實施詐騙行為，不應因此承擔結果責任。

5. 已設有防詐騙警示機制，原告應有警覺義務：被告神腦公司指出，其平台交易流程已常態性附帶防詐提醒，諸如訂購成功通知、電子報等均載有警語。銀行業者亦普遍於網銀系統中提醒防詐資訊。原告未能警覺，係因個人不慎誤信詐騙手法，與平台無涉。

6. 原告主張精神損害無具體證明，不符請求要件：原告請求 2 萬元之非財產上損害精神慰撫金，惟並未提出任何精神受創之診斷證明或其他證據，亦未證明損害達個資法第 28 條第 2 項所謂「非財產上之損害」之標準，難以構成請求要件。

7. 法律請求構成混淆，援引規範不符：個資法第 29 條第 2 項已為民法第 195 條之特別規定，原告若依個資法請求非財產上損害，即不得再併行主張民法第 184 條或 195 條。其援引法條混淆，請求應屬無理由。

二、法院判決理由分析[92]

(一) 李文正是否構成共同侵權並負損害賠償責任：法院於本案中就李文正是否應負損害賠償責任進行實質審查，認為依據民法第 184 條第 1 項及第 185 條規定，數人共同不法侵害他人權利者，須負連帶損害賠償責任。原告主張其因誤信詐騙話術而於短期間內匯款共計 59 萬 9,963 元，且李文正係詐騙集團成員，擔任取款車手並實際領取上開款項。法院審酌台北地檢署多份起訴書所載事實，足認李文正參與詐騙並從事資金收取行為，構成共同侵權行為，法院遂認原告該部分請求有理由，予以准許。惟就原告另主張遭詐騙匯款之 9 萬 9,552 元部分，雖提出轉帳及通話紀錄為佐證，惟原告未能證明該筆匯款與李文正所屬詐欺集團具關聯性，亦坦承無其他佐證資料，致法院無法建立加害人身份與

[92] 臺灣臺北地方法院 112 年度訴字第 2854 號民事判決。



doi:10.6342/NTU202501770

因果關係，認原告該部分主張欠缺舉證基礎，應予駁回。

(二) 關於原告主張被告神腦公司與林榮賜應負連帶賠償責任之審查：法院首先指出，依民事訴訟法第 277 條，原告如主張被告神腦公司違反個資法第 27 條、第 29 條，應就其個資係由被告神腦公司洩漏，且被告神腦公司未採行適當安全措施兩層事實負舉證責任。即便個資法對故意或過失採反證推定，該推定僅及於主觀歸責，原告仍負有初步證明外洩事實與資安缺失之義務。法院認為原告未能完成此一舉證責任，應駁回其對被告神腦公司及林榮賜之請求。

(三) 原告未能證明被告神腦公司為個資洩漏來源及與詐騙間之因果關係：原告曾於系爭平台交易，確實留下個資與信用卡資訊，惟該交易亦涉及統欣生技公司及台北富邦銀行，詐騙手法則係冒用銀行人員名義進行誤導。法院認為在多方參與與多重資訊流通下，原告無法排除其個資可能由他方洩漏，自難論證資料係由神腦公司所外洩，亦無法導出被告神腦公司未採資安措施與原告損害間之相當因果關係。

(四) 高風險賣場資料與防詐公告無從證明神腦公司違法：原告引用刑事局公告神腦平台為高風險賣場及其他消費者曾遭冒用情形，試圖證明被告神腦公司資安疏漏。惟法院指出該公告時間與原告實際交易日並不重疊，無法據以推論原告個資外洩源頭。同時，被告神腦公司於購物頁面設有具體防詐警語，明確提醒消費者勿依指示操作 ATM 或提供個資，法院認其已盡告知義務與最低風險控管措施，難認有違反個資法情事。

(五) 被告神腦公司提出資安制度佐證其已善盡保護義務：法院審酌被告神腦公司提出之完整資安管理機制，包括個資保護章程、事件處理流程、紅隊演練報告等，並指出其網站經複測為低風險，顯示被告神腦公司對資安已有基本維護。即使原告指出 165 反詐騙專線期間曾接獲 121 件冒用被告神腦公司名義詐騙之通報，法院仍認該事實僅能證明詐團利用被告神腦公司名義行騙，並不當然代表被告神腦公司平台即為資料外洩源。綜上，原告對被告神腦公司及林榮賜所提財產與非財產損害賠償請求，應予駁回。

三、判決影響與未來發展之分析

(一) 企業責任之舉證門檻與因果鏈條認定：相對於詐騙行為人責任的肯認，法院對



doi:10.6342/NTU202501770

企業（神腦公司）是否應負外洩致詐損之責則採取相當嚴謹之審查標準。法院指出，個資法第 29 條雖設有「過失推定」規定，但此推定須建立於原告初步證明「個資確係由被告洩漏」與「被告未盡資安義務」兩要件基礎上。倘若原告無法合理排除資料係從其他交易環節（如銀行、物流業者等）洩漏，則無從推定企業為外洩來源，亦無由認定其有過失。法院未採「結果倒推」或「資料具關聯性即有責」之邏輯，而堅持資料來源需具體可證，顯示對因果關係之舉證採取保守態度。此舉固有助控管濫訴風險，惟在資訊不對等背景下，對原告舉證能力要求恐過於嚴格，亦引發實質保護落差之疑慮。

(二) 資安合規不再止於「制度存在」，而重於「制度落實」：雖最終未判企業有責，法院仍詳細檢視被告神腦公司提出之資安措施，包括資安政策、紅隊演練報告、事件通報紀錄、個資管理辦法等，並明確指出：「企業是否能提出完整且有效落實之紀錄，將成為法院審理過失與否的核心依據」。此意涵在於企業無法僅以「有制度」抗辯責任，而須證明「制度有效運作」。未來企業面對類似訴訟時，需準備具體可查驗之紀錄文件，包含資安異常應變流程、第三方稽核報告與員工操作紀錄，否則即便資安制度完備，亦可能被認定「未盡注意義務」。

(三) 詐騙行為可能成為因果關係之中斷事由：法院進一步指出，詐騙集團係藉冒名手段誘騙被害人轉帳，其行為屬積極獨立之違法行為，有可能中斷企業過失與財損之因果關係。該見解為實務上釐清企業與第三方詐騙間責任邊界提供清晰基準。未來若企業已建立合理防護機制，且詐騙手法獨立於企業所控制之資訊流，則企業可主張詐騙行為為「介入原因」，不負相當因果責任。此見解對企業有利，也將促使企業建立更完備之「防詐聯防體系」，以證明其對第三方犯罪行為已採取合理預防作為。

(四) 本案亦凸顯個資法第 27、29 條於實務適用上的制度性困境。多數消費者缺乏資安技術背景與蒐證資源，難以釐清資料於企業內部流通、處理與外洩的過程，若仍要求其完全承擔舉證責任，將削弱個資法保障資訊自主與人格權的立法初衷。為因應資訊不對等與證據偏在的現實挑戰，未來制度發展可考慮從四方面強化：其一，導入「外洩來源推定制度」，仿效歐盟 GDPR 第 82 條之設



doi:10.6342/NTU202501770

計，於企業明確持有個資的前提下，推定其為可能外洩來源，由企業負反證責任；其二，建立「資料鏈追蹤機制」，透過資料指紋技術與跨機關合作，實現個資流向監測與外洩溯源；其三，明文化舉證責任轉換原則，透過修法或釋法將推定過失條款具體化，以減輕受害者舉證負擔；其四，強化「集體訴訟協助制度」，集中資源、統一鑑識標準，提升消費者求償成功率。總結而言，本案雖最終僅對詐欺行為人判決成立民事責任，駁回對企業之請求，然法院對個資保護責任鏈條、舉證配置與企業資安義務的具體分析，已為未來類似案件奠定重要司法基礎。面對日益擴張的數位詐騙與資訊風險，企業唯有建構完整、可驗證的資安制度，方能在實務中站穩立場，避免承擔擴張性法律風險，亦有助於推動個資保護與產業發展之間的制度平衡。

## 第十一項　三商行股份有限公司個資外洩案

裁判字號：臺灣臺北地方法院 111 年度北簡字第 16345 號民事判決

一、案件事實

(一) 原告起訴主張：原告於 111 年 8 月 19 日於鞋全家福蘆二店購鞋，並依店員建議填寫個人資料加入會員，以享有優惠，並以國泰世華信用卡刷卡消費 1,031 元。嗣於同年 9 月 6 日，原告接獲冒稱鞋全家福及國泰世華員工之詐騙電話，對方能具體述及前述消費資訊，並以「入帳錯誤」及「需解除設定」為由，誘使原告依指示匯款，致遭詐騙共計 299,988 元。被告早已知悉其消費者資料遭冒用進行詐騙事件頻繁發生，且曾被刑事警察局列為高風險賣場，然僅於官網發布防詐公告，未於實體門市加強宣導或由店員進行口頭提醒，亦未採有效防範措施。原告認為，被告未盡個資法所要求之適當安全維護義務，導致原告個資外洩並蒙受損害。因此，原告依個資法第 12 條、第 27 條、第 28 條第 2 項、第 29 條及消保法第 7 條，請求被告賠償 35 萬元（含精神慰撫金 5 萬 12 元），並自起訴狀送達翌日起至清償日止，按年利率 5%計算利息。

(二) 被告抗辯：原告雖稱遭詐騙，然未提出足以證明其主張之具體證據，且即使原告所述屬實，亦無法直接證明詐騙集團係使用自被告處洩漏之個人資料為詐騙手段，故難以成立被告對個資外洩負有責任。另就防範措施部分，被告指出，其已於 111 年 8 月 27 日及 29 日，分別於官方網站首頁及 Facebook 粉絲專頁



doi:10.6342/NTU202501770

刊登防詐騙公告，並於同年 9 月 1 日發送簡訊提醒所有會員注意詐騙風險。然原告仍於 9 月 6 日遭詐騙，應係其個人未善盡注意義務所致，與被告無涉。被告並強調，其已盡善良管理人之注意義務，維護會員個人資料安全無虞，原告請求賠償並無事實與法律上依據，請求法院駁回原告之訴。

二、法院判決理由[93]

(一) 舉證責任與侵權責任成立之法律要件：法院指出，當事人主張有利於己之事實者，即有舉證責任。依個資法第 12 條、第 27 條及第 29 條，非公務機關若違法導致個資遭不法蒐集或洩漏，即負損害賠償責任，但若證明無故意過失則免責。另依民法第 184 條，侵權責任成立需具備故意或過失之加害行為、損害結果，以及兩者之間具相當因果關係等要件，若欠缺任一要件即不構成侵權責任。此外，儘管個資法設有故意過失推定條款，但原告仍須舉證證明其個人資料確實遭到不法蒐集或利用。因此，本案原告須舉證證明被告公司確實有外洩其個資之行為，且與原告之受損害結果具因果關係，始能主張侵權行為責任。法院認定，原告就前述各項事實之舉證責任並未免除，應負擔完整的舉證義務。

(二) 原告主張受詐騙事實經查證為真實：法院查明，原告主張其於鞋全家福蘆二店刷卡消費並加入會員，之後遭假冒鞋全家福員工之詐騙集團成員以電話詐騙方式騙取近 30 萬元之事實，經檢視警察局報案紀錄及新北地檢署偵辦案件資料，以及新北地方法院刑事判決卷宗核實後，確認原告所述之遭詐騙過程確實發生，且該詐騙行為已受到刑事司法機關認定，並據法院核對該等刑事相關資料無誤，堪信為真實。然而，法院也特別強調，原告遭受詐騙之事實真實存在，並不代表詐騙行為與被告公司之行為間具有必然之法律上因果關係。原告仍需就詐騙集團取得其個資之管道與被告公司之責任間的連結進行舉證，方能確立法律上的損害賠償責任。

(三) 原告未能證明個資洩漏源自被告公司：法院指出，原告雖有提供消費發票、存

[93] 臺灣臺北地方法院 111 年度北簡字第 16345 號民事判決。



doi:10.6342/NTU202501770

摺明細、報案紀錄等證明其消費及遭詐騙事實，但該等證據僅能證明其曾在被告門市消費及確有遭詐騙情形，無法證明系因被告公司洩漏其個資所致。此外，被告提出證據證明其門市顧客刷卡資料係透過遠傳電信 MPLS VPN 封閉網路傳輸，加上信用卡中心對刷卡資訊進行隱碼處理，被告無從獲悉完整卡號及銀行資訊；同時，被告已落實資訊安全措施如防火牆、防毒軟體及資料去識別化處理，並具完善個資保護政策及教育訓練。因此，法院認定原告未能合理排除個資遭洩漏係發卡銀行或信用卡中心等其他環節所導致之可能性，亦未能舉證被告確有洩漏行為或保管不當之過失行為存在。

(四) 被告已盡合理之防詐騙告知義務：法院查明，被告公司針對詐騙情勢，早在原告受詐騙之前，即於官網及社群平台公告反詐騙提醒，並對會員（包括原告）發送防詐騙簡訊通知。法院認定，被告已透過多種管道適時提供防詐騙資訊，合理履行消費者個資安全告知之義務。原告雖主張因手機安全程式設置因素未見提醒簡訊，但法院認為此非被告過失所致，係原告自身設置所致，因此無從歸責於被告。此外，原告主張網路其他消費者亦受害並不能證明自身個資即為被告所洩漏，故法院認定原告主張被告未盡合理防範或警示義務之抗辯理由不足，難以採信。綜合而言，被告對於防堵詐騙措施已有合理盡力，尚難認被告在本案中有任何顯著之過失責任。

(五) 本案不適用消保法第 7 條之賠償責任：法院強調，依據消保法第 7 條，企業經營者須保證其提供之商品或服務安全且符合專業水準，但本案爭議之個人資料保存行為本身，並非屬企業提供之商品或服務內容，而係附隨於消費過程之間接義務，故不符合消保法第 7 條適用之要件。此外，原告也未能證明所受詐騙損害係來自於被告公司之個資外洩行為，故難以依消保法主張被告公司負賠償責任。換言之，本案所涉個資保管義務雖與消費有關聯性，但並非直接提供消費服務之範疇，消保法所規範之責任範圍並未及於本案之情形。因此，法院最終駁回原告依消保法主張之損害賠償請求。

(六) 綜合上開判斷，法院認為原告無法就個資洩漏來源、被告安全措施疏失、損害與過失行為間因果關係等構成要件完成舉證，被告公司亦已建立具體之資訊安全制度及防詐宣導，故不構成個資法或民法上之損害賠償要件。另消保法亦



doi:10.6342/NTU202501770

不生適用，原告請求全數駁回。

三、判決影響與未來發展之分析

本案係個人資料外洩引發之詐騙損害賠償案件，法院最終判決原告敗訴，認定其未能證明個資係自被告外洩，亦無證明被告資訊安全有疏失，致與其財產損害間具相當因果關係。此判決體現目前法院在個資法損害賠償構成要件、舉證責任與企業合規義務上之實務操作，對當前頻繁發生之個資爭議與數位詐騙風險，具指標性影響。

(一) 法院對個資法第 29 條「推定過失責任」適用之限制

雖個資法第 29 條明文採「推定過失責任」，本案法院仍採嚴格要件審查，要求原告先證明資料確係遭被告不法蒐集、處理或利用後，始能進一步適用該條款。換言之，法院未採「資料外洩即推定企業有責」之見解，而是強調個資外洩來源須由原告具體證明，否則舉證失敗即駁回請求。此舉固有助防範濫訴與不當轉嫁企業風險，但對受害者而言，舉證門檻明顯偏高，可能形成法律保障與實質救濟之落差。

(二) 個資來源舉證責任之嚴格要求與制度困境

本案法院明確表示，僅因詐騙者掌握特定交易資訊，尚不足以推定該資料係由被告洩漏，並指出該資料可能來自多個資訊傳輸環節，如電商平台、第三方金流、物流業者等。此判斷模式，實際上要求原告具備資安鑑識能力或取得資料流通鏈條的存取紀錄，方能主張損害與特定企業間存在因果關係。然而，現行制度下並無揭露義務或舉證協助機制，被害人難以獲取關鍵事證，致訴訟成功機率大幅降低。未來若不建構「合理推定」制度與揭露義務，類案多將面臨舉證失敗之風險。

(三) 企業資安合規責任的舉證模式與法院期待

法院詳列被告所主張之資安作為，如 MPLS 封閉網路、SSL 加密傳輸、防火牆、資訊分層遮蔽、員工教育訓練與保密協定等，並以此為基礎認定其已符合當時科技及行業專業標準下之合理期待。此判斷標準趨向形式審查，即「企業如能提出資安 SOP、合規紀錄、第三方稽核報告等，即得推定無過失」。在舉證責任未轉換前提下，法院多半接受企業所提出之管理制度或技術證明，導致即便發生實際個資外洩，亦難構成賠償責任。此一趨勢顯示，未來若無法建立「反證責任轉換」或「風



doi:10.6342/NTU202501770

險比例原則」等操作機制，受害者將持續處於資訊弱勢。

(四) 消費者保護法適用範圍之限縮與疑義

法院另認為，本案原告僅提供個資註冊帳號，未直接支付對價，因此不構成消保法第 7 條所稱「消費者」與「交易行為」，難以主張消費者保護法下之企業安全注意義務。然此見解未充分反映數位經濟中「資料即對價」的事實。現今電商與平台模式普遍藉由收集個資進行再行銷、個人化推播及異業合作，實質上已將個資納為商業價值來源。若法院持續限縮消保法保護範圍，將排除大量依靠個資交換經濟模式運作之企業責任，與現代商業結構與消保立法精神恐不相符。未來應透過法釋或修法，明確肯認「資料提供＝經濟對價」之概念。

(五) 制度發展方向：從個案解決邁向結構改革

本案顯示，在現行制度下，個資受害者若無取得資安紀錄之管道，恐難舉證成功。為回應資訊不對等與責任鏈模糊問題，未來應思考下列制度改革方向：

1. 建立資安揭露與調查義務：如主管機關建置資安事件揭露平台，企業須主動公告外洩事實與受影響範圍。
2. 導入舉證協助或舉證責任轉換制度：借鏡歐盟 GDPR 第 82 條損害賠償規定，對資料控管者設立明確反證義務。
3. 強化集體訴訟機制：鼓勵受害者透過團體訴訟集中資源、統一舉證，降低單一當事人之訴訟風險與成本。
4. 建立高風險行業主動稽核通報義務：針對電商、票務、金融與交通等高敏感度產業，要求定期公開資安稽核報告。
5. 本案判決顯示法院重視企業合規努力，亦對資安管理作出制度化審查，但在舉證責任、因果關係與消費者保護的適用上，採取保守立場，對個資受害者並不友善。未來欲實現個資法保障資訊自主與人格權之立法目的，應從「舉證責任重分配」、「消費關係認定」及「制度性資料揭露」等方向，進行實質改革。

## 第十二項　統聯汽車客運股份有限公司個資外洩案

裁判字號：臺灣新北地方法院 112 年度重小字第 3188 號民事判決



doi:10.6342/NTU202501770

一、案件事實

(一) 原告起訴主張：原告於 112 年 5 月 13 日前某時利用被告統聯汽車客運股份有限公司（下稱統聯公司）提供之網路訂票服務訂購車票，嗣於同年 5 月 13 日 20 時 31 分許，在住所接獲自稱被告客服人員之來電。來電人能準確敘述原告姓名、身分證字號、訂票日期、發車時間及起訖站等細節資訊，並稱因操作疏失導致多訂二十餘張車票，需通知郵局人員協助解除錯誤訂單。隨後原告即接獲另一自稱郵局人員之來電，要求原告操作網路銀行密碼以「解除扣款」。原告信以為真，依指示操作網銀分別輸入「解鎖密碼」與「關閉密碼」，結果遭詐騙合計 82,276 元。雖無證據顯示被告有意洩漏個人資料，惟作為資料蒐集及管理者之被告統聯公司未盡其對個人資料之安全保護義務，致原告資料外洩，為詐騙者所利用，造成財產上損害。原告遂依個資法第 29 條第 1 項規定，請求被告統聯公司賠償財產上損失 82,276 元，並自起訴狀送達翌日起至清償日止，按年息 5%計算利息。

(二) 被告統聯公司抗辯：被告請求駁回原告之訴，主張其已依據資訊安全標準採取相當之個資保護措施，包括採用居易科技股份有限公司製造之 DrayTek Vigor2910 防火牆設備，具備內容安全與策略安全雙重防護功能，如即時通訊與點對點服務屏蔽、NAT 埠管理、DMZ 隔離、DoS/DDoS 防護、系統日誌紀錄及 IP/MAC 綁定等機制。此外，被告統聯公司所使用之網路與金流服務亦皆採用 SSL-TLS1.2 以上等級之傳輸加密，足證其已盡合理安全維護義務，並無故意或過失。原告之財損係由第三人詐騙行為所生，與被告統聯公司訂票系統並無相當因果關係。即使原告受有損害，該等詐騙係因原告個人輕信來電操作銀行系統所致，且原告為成年國立大學學生，應具備基本資訊安全意識，卻未加警覺，對損害結果自應負有過失責任，難認被告統聯公司應負損害賠償之法律責任。



doi:10.6342/NTU202501770

二、法院判決理由[94]

(一) 被告未盡適當安全維護義務而有過失：依個資法第 27 條與第 29 條規定，非公務機關如未採適當安全措施致個資外洩，應負損害賠償責任。第 29 條明定「推定過失責任」，即一旦原告主張其個資遭外洩且提出初步證據，即推定被告有過失，被告須負舉證責任，證明其已無故意或過失，方能免責。本案中，雙方不爭執原告曾將個資交付被告統聯公司，亦不爭執曾有外洩事實，故舉證責任已轉移至被告統聯公司。被告統聯公司雖主張使用 DrayTek Vigor2910 防火牆及 SSL-TLS1.2 憑證，已盡防護義務，然法院認該防火牆為 2006 年產品，事件發生時已逾 16 年，未符合資安設備應隨技術更新之常態，難認其能有效防堵網路攻擊。被告統聯公司亦未提出其他積極證據證明其資安制度完備，無從舉證其無過失。綜上，法院認定被告統聯公司未採適當資安防護措施，依法推定其有過失，舉證責任未盡，應負賠償責任。

(二) 被告過失行為與原告損害間是否具因果關係：

依民訴法第 277 條但書規定，當事人雖應自行舉證，但若法律另有規定或「顯失公平」，得減輕舉證責任。該但書於 89 年修法增設，係因傳統與現代訴訟型態複雜，尤其涉及公害、製造責任、醫療糾紛等類型，若嚴格依原則舉證，往往導致被害人無法獲救濟，違反正義原則。法院應視案件性質、公平原則、證據偏在、蒐證困難、證明因果關係之難易、雙方舉證能力差異及法律設計不足，適用但書規範。

本案原告依個資法第 29 條請求損害賠償，須證明被告統聯公司違法持有個資致外洩且與自身受害有相當因果關係。然而網路資安技術複雜，牽涉駭客與詐騙等多重因素，被害人實難掌握完整事證；相對地，被告統聯公司作為收集、使用個資之經營者，對外洩風險有控制與分擔責任，舉證能力亦優於原告。法院因此比照公害訴訟之實務見解（最高法院 103 年度台上字第 1311 號、102 年度台上字第 31 號判決），認被告統聯公司行為所形成之危險已具「相當合理確定性」，應推定原告之損害與被告統聯公司過失間具一般因果關係。故除非被告提出具體可推翻該因果

[94] 臺灣新北地方法院 112 年度重小字第 3188 號民事判決。



doi:10.6342/NTU202501770

關聯之反證，否則法院應推定其存在。本案被告僅出示媒體報導，不能有效排除因果關係，亦未提出其他反證，無法具體證明其個資洩漏與原告損害間無關，法院因此肯認因果關係成立。

(三) 原告是否有與有過失？法院是否應減輕賠償責任？

法院指出，雖原告因個資外洩受詐騙導致財產損失，但原告為成年且具高等教育背景，應對常見詐騙手法具警覺，惟其未進一步查證即依來電指示操作網銀輸入密碼，難謂無過失。法院認為原告未妥善自我保護，對損害之發生亦有一定責任，應適用民法第 217 條減輕賠償責任。綜合考量，法院評定原告過失比例為三成，被告統聯公司過失比例為七成，故原告可得賠償金額為 57,593 元。

三、判決影響與未來發展之分析

法院判決統聯汽車客運公司對個資保護未盡注意義務，並推定其與原告損害間具因果關係，應負七成賠償責任，具備以下數點實務意涵與制度發展可能性：

(一) 推定過失與資安防護義務之具體化

法院明確指出，依個資法第 29 條規定，一旦個資確有外洩且原告受有損害，即推定非公務機關有過失，舉證責任反轉，由企業負責證明其已盡資安防護義務。此一見解延續我國實務對個資侵權舉證負擔調整的立場，有利降低受害者於技術資訊高度不對稱下的舉證難度。更值得注意者，法院並未僅以企業宣稱「使用防火牆」即認為已盡保護義務，而是進一步審查其設備更新情形與防禦效能。法院認定統聯仍使用 2006 年出產之舊型防火牆，未符現代資安威脅防禦需求，故難認其已採「適當」安全措施。未來法院可能會更加著重於企業是否落實持續更新機制、是否有定期資安稽核及事故應變計畫，而非僅形式上宣稱使用加密傳輸或硬體設備。

(二) 舉證責任與因果關係之實質推定

在因果關係認定部分，法院援引民訴法第 277 條但書，並比照公害訴訟、醫療糾紛及製造物責任等案件，認為在科技高度專業化、證據偏在之個資外洩案件中，應採「危險領域理論」或「合理危險確定性」之推定模式。本案即採最高法院 102 年度台上字第 31 號及 103 年度台上字第 1311 號判決之精神，認企業行為所產生之資訊風險已達足以造成損害之程度，故可推定其與損害間具備一般因果關係。



doi:10.6342/NTU202501770

此一見解對未來數位時代個資侵權訴訟具有指標意義。傳統條件理論要求精確證明「若無被告行為即無損害結果」的邏輯鏈，在現代資安侵害中顯不合時宜，尤其是駭客攻擊、資料轉賣與跨平台詐騙串聯案件中，被害人難以掌握細節。未來法院勢必持續以「相當因果關係」之推定與反證方式處理此類新型損害類型。

(三) 對消費者過失的合理衡量與過失相抵

法院雖支持原告請求，但也依民法第 217 條認定原告對詐騙事件應具備基本警覺性，原告未查證即聽從詐騙指示，輸入所謂「密碼」而致財產損害，應負部分過失責任。法院綜合考量後，裁定原告負 30%、被告統聯公司負 70%，反映出法院對受害者自我防衛義務仍保有一定期待。

此項認定展現司法對消費者保護與責任衡平的雙重要求：一方面肯認企業資安義務為首要防線，但另一方面也提醒民眾應具備基本的反詐騙知能。對企業而言，這也提示應加強風險預警與用戶教育，例如：即時通報異常登入、簡訊示警或設計防範社交工程誘導的操作介面。

(四) 本案對未來個資外洩案件處理模式具有以下幾項深遠影響

1. 促進企業資安標準化與合規實踐：防火牆規格、系統更新頻率將不再是企業內部行政問題，而直接關係法律責任。企業若使用明顯過時的資安設備，即可能構成推定過失。
2. 強化受害人救濟機制：法院接受因果關係推定標準，降低受害人證明負擔，將促使企業在事前加強內控，而非事後以證據不足為由推卸責任。
3. 司法認定與產業風險轉移：本案承認企業對個資外洩風險之控制優勢，有助於促進保險業或資安服務產業的進一步介入。未來，法院可能更重視企業是否有投保資安責任險、是否委外專業第三方進行滲透測試與資安稽核。
4. 立法政策參考：本案所呈現之司法技術與因果推定模式，亦可作為未來個資法修法方向之參考，考慮引進明示性「舉證責任轉換條款」、技術標準附則或企業安全認證制度。統聯案判決具體呈現我國法院對資安與個資保護責任日益嚴謹的審查態度，也體現數位社會下司法對技術不對等所帶來舉證困境的回應策略。此判決不僅提供實務操作的參考依據，更將引導企業在數位時代重塑其個



doi:10.6342/NTU202501770

資治理思維，落實「從紙本合規走向動態風險治理」的趨勢。

## 第二節　我國法院判決差異分析

### 第一項 判決差異概述

透過對我國十二件與電商平台個資外洩相關之民事訴訟判決進行系統性比較，可發現法院在責任判斷各構成要件上呈現顯著差異，尤其在「個資來源認定」、「過失與資安義務審查」、「相當因果關係判準」、「消費者本身過失考量」之面向，展現出實務上標準尚未統一的現象，對於企業法律風險預測與個資保護制度之可預期性構成挑戰。

首先，在個資來源是否可歸責於業者方面，部分案件如橘熊科技案、威尼斯案與統聯客運案，法院基於證據偏在與事實整體推論，採取「來源推定」認定資料外洩係由業者系統所致。然而，包括雄獅旅行社 108 年案、神腦國際案、iRent 案與三商行案在內，多數判決仍要求原告須提出具體證據證明資料確由被告外洩，未達舉證門檻即遭駁回。此種高舉證門檻對資訊不對等的消費者而言，顯然造成權利實現的障礙。

其次，就業者是否有過失之判斷，多數法院援引個資法第 29 條「過失推定」原則，認定若業者未能提出具體資安實施紀錄或內部查核報告，即可推定其未善盡適當安全維護措施。判決如迪卡儂案、北投麗禧案二審與威尼斯案即明確指出，業者雖主張制度設計完備，然未能舉證落實情形，應負資安過失責任。相對地，雄獅旅行社案、三商行案與神腦案等則因業者實際執行資安政策並有具體證據佐證，法院認無過失，免除其賠償責任。

在因果關係判斷方面，實務多採取嚴格標準，將詐騙行為視為第三人介入所致，可能中斷業者與財損間之因果鏈。例如，iRent 案、神腦案與王品二審案皆否定因果關係成立，主張即使外洩發生，仍難證明詐騙損失係可歸責於被告。然而亦有例外，如橘熊案、統聯案與威尼斯二審，法院認為在集體受害、特定詐騙手法與時序緊密等情境下，業者應預見詐騙風險，進而推定因果關係存在，並容許調整舉證責任分配。

至於被害人自身是否有過失之評價，部分判決如統聯案、威尼斯案與迪卡儂



doi:10.6342/NTU202501770

案，明確指出原告對詐騙手法未盡查證義務，故就財損部分須自負一定比例責任（例如負擔三至九成不等），反映出法院在衡量雙方行為責任時採取比較過失原則。而王品案亦指出原告在接獲假冒客服電話後仍提供重要資料，行為欠缺注意，應自負損害後果。

綜上所述，雖我國法院普遍援引個資法體系進行法律適用，然在個案認定上尚缺乏一致性與明確標準，導致實務運作結果分歧。此不僅使企業難以預判法律風險，也使被害人維權門檻提高，有必要從制度設計與司法解釋層面進行強化與統一，以促進個資保護責任的穩定與公平。

【表 2】 我國法院判決比較表

| 案件名稱與判決字號 | 個資來源是否來自業者 | 業者是否有故意/過失 | 財損與業者行為間因果關係 | 被害人是否有過失/非財產損害 |
|---|---|---|---|---|
| 橘熊科技(OB 嚴選)<br>【士林地院 107 湖小 401】 | 法院推定來源為業者。 | 推定未善盡保護義務，存有過失。 | 認定有相當因果關係。 | 未明確指出被害人過失。<br>判賠非財產損害 2 萬元。 |
| 雄獅旅行社 107 年案<br>【士林地院 107 消 6】 | 未證明個資來自業者。 | 無過失，已落實完備資安制度並實際執行。 | 駭客入侵係外力介入，非業者可歸責，無因果關係。 | 部分受害人有過失。<br>駁回非財產上損害 |
| 雄獅旅行社 108 年案<br>【士林地院 108 湖小 558】 | 未證明個資來自業者。 | 已盡資安與通知義務，無過失。 | 法院認為原告財損係其輕信詐騙電話所致，無因果關係。 | 原告之訴駁回。原告未請求非財產上損害。 |
| 王品瘋美食 App<br>【臺中地院 110 中簡 1952、112 簡上 120】 | 一審認定個資外洩係來自業者平台；<br>二審認定無足夠證據證明資料外洩來自業者。 | 一審認定有過失，未善盡資安義務；<br>二審認定業者已提供適當資安措施，無過失。 | 一審認定有因果關係。<br>二審否定因果關係。 | 原告有過失，<br>一審就非財產損害判業者賠償 2 萬元，財損未予賠償。<br>二審全部駁回。 |
| 北投麗禧酒店<br>【臺北地院 111 訴 5578、高院 112 上 656】 | 認定被告系統遭第三人不法竊取，個資外洩自業者系統。 | 一審認無過失，二審認有過失。 | 無相當因果關係，損害係第三人詐騙所致。 | 肯認非財產損害成立，判賠 2 萬元。 |
| 中華民國運動神經元疾病友協會 | 未證明個資來自業者。 | 無證據違反資安義務。 | 無因果關係。 | 原告之訴駁回。<br>無認定非財產損 |



doi:10.6342/NTU202501770

| 案件名稱與判決字號 | 個資來源是否來自業者 | 業者是否有故意/過失 | 財損與業者行為間因果關係 | 被害人是否有過失/非財產損害 |
|---|---|---|---|---|
| 【臺北地院 111 北簡 1007、111 簡上 266】 | | | | 害。 |
| 威尼斯國際事業<br>【新竹地院 111 竹東簡 48、112 簡上 143】 | 法院推定來源為業者。 | 未盡適當安全措施，構成過失。 | 一審認無因果關係。<br>二審認有因果關係。 | 被害人與有過失(原告負 7 成責任)。<br>原告未請求非財產上損害。 |
| 迪卡儂案<br>【臺中地院 111 訴 2708、臺中高分院 112 上易 208】 | 法院認定來源為業者。 | 未盡適當安全措施，構成過失 | 一審認有相當因果關係。<br>二審否定因果關係。 | 一審認定原告與有過失(原告負擔 9 成責任)。<br>二審僅判賠非財損 2 萬。 |
| iRent 案<br>【臺北地院 112 訴 3711、高院 113 上易 471】 | 未能具體證明個資來源為業者。 | 行政處分撤銷，法院認無過失。 | 無因果關係。 | 無認定非財產損害。 |
| 神腦國際<br>【臺北地院 112 訴 2854】 | 未證明個資來自業者。 | 未證明業者未採行適當安全措施。 | 未證明個資洩漏來源與詐騙間之因果關係。 | 駁回原告請求。 |
| 三商行（鞋全家福）<br>【臺北地院 111 北簡 16345】 | 未證明個資來自業者。 | 已落實資安，無過失。 | 未能證明因果關係。 | 駁回原告請求。 |
| 統聯汽車客運<br>【新北地院 112 重小 3188】 | 認定來源為業者。 | 推定過失，業者未能反證。 | 法院推定有因果關係。 | 原告與有過失，(原告負擔 3 成責任)。<br>無請求非財產損害。 |

## 第二項 法院主要認定準則

臺灣法院在審查個資外洩案件時，主要依據「民法」及「個資法」規定來認定侵權行為是否成立，並從以下幾個方面進行審查：

### 一、侵權行為成立要件

根據民法第 184 條第 1 項前段，構成侵權行為必須滿足：行為人具有故意或過失、其行為不法侵害他人權利，並且該不法行為與損害之間存在因果關係。個資



doi:10.6342/NTU202501770

外洩案件中，原告必須證明企業因違反個資保護義務而使個人資料遭不法利用，並進而導致具體損害的發生。

二、過失責任與違法性

除了證明故意或明顯過失之外，法院也會探討企業是否違反法定義務，未採取足夠安全措施，從而構成違法行為。根據個資法第 27 條，企業必須採取適當的技術及管理措施，防止個資遭竊取或不法利用；若因此發生外洩，即可能被推定存在過失，除非企業能舉證證明其無故意或重大過失。

三、相當因果關係的認定

判斷企業行為與消費者損害之間是否構成相當因果關係，是本類案件的核心難題。法院會綜合考量當事時存在的環境因素、技術漏洞、第三人介入等多種因素，來判斷企業的行為是否為損害發生的不可或缺條件。若在一般情形下，存在該條件則可能導致相同結果，則可認定為相當因果關係；反之，若認為該條件僅屬偶然或非必要因素，則不構成直接因果關係。

四、舉證責任分配

由於資料外洩事件涉及高度技術性證據，消費者在證明資料外洩與損害間直接連結時常面臨重大困難。部分判決採取降低原告舉證責任的方式，參照公害訴訟模式，反而要求企業舉證其安全措施已達標準，或提供反證以否定因果關係；而另一些判決則仍要求原告對所有關鍵事實負舉證責任，這直接影響了判決結果的走向。

## 第三項 因果關係與舉證責任

一、因果關係的認定問題

個資外洩案件中，如何確認企業行為與消費者損害之間存在直接且必然的連結，成為審理的難點之一。有些判決中，法院認為企業違反安全措施的行為足以推定資料外洩與損害存在相當因果關係；例如，在臺灣新北地方法院 112 年度重小字第 3188 號案件中，法院指出被告無法證明資料外洩與原告損害間不存在因果關係，故支持原告請求。另一方面，也有判決認為，個資外洩本身並非必然導致消費者遭受詐騙或其他損害，若第三人（如詐騙集團）的故意介入，則可能中斷企業行為與



doi:10.6342/NTU202501770

損害之間的直接連結，從而不構成企業的直接責任。臺灣臺中地方法院 110 年度中簡字第 1952 號判決即採取此觀點，認為詐騙集團的介入是導致損害發生的主要原因，企業因此不應承擔全部賠償責任。

二、舉證責任分配的爭議

在我國個資法第 29 條規定中，對於非公務機關因違反法定義務而致當事人個人資料遭不法蒐集、處理、利用，或其他方式侵害其權益者，明定應負損害賠償責任。雖法條明文允許非公務機關於能證明其無故意或過失時免責，惟此舉證責任之分配，實質上已形成一種「推定過失責任」制度。亦即，當個資外洩事實發生後，若企業未能提出反證證明其已盡善良管理人之注意義務，則應推定其具有過失，須對當事人所受損害負賠償責任。

此舉證責任的安排，主要考量消費者在個資外洩事件中，處於資訊不對等的劣勢地位。尤其在涉及企業內部資訊安全機制、人員控管流程等高度專業與技術性之事項時，外部當事人難以自行取得足以證明企業違法或疏失的直接證據。此外，關於個資是否實際遭到不法利用、是否造成具體損害，以及兩者之間是否存在相當因果關係等問題，亦屬高度不確定且難以舉證的事項。基於此一證據偏在與舉證困難的現實情況，學理與實務普遍主張應由企業承擔反證責任，證明其已採取適當安全保護措施，並與個資外洩損害無因果關係，以維護當事人之司法救濟權利與程序正義。

事實上，該等舉證責任之倒置與重新分配，亦可觀察於其他訴訟類型中之發展趨勢，如公害訴訟、產品責任及醫療過失案件等，其共通特徵在於：加害行為人掌握關鍵資訊，而被害人卻難以提出具體證據。為避免傳統民事訴訟法第 277 條「誰主張，誰舉證」原則造成不公平結果，法院常以實質正義為導向，對舉證責任加以調整。此一趨勢亦為個資外洩事件之法律處理提供重要借鏡。

我國部分法院判決已開始採取類似公害訴訟中的「因果關係舉證責任緩和」作法，在消費者無法證明個資外洩與損害之間存有直接連結時，轉而要求企業提出具體說明其已盡防護義務。此舉一方面有助於補充現行法制在舉證分配上的不足，另一方面亦促使企業重視資訊安全治理責任。然而，此一發展亦引發爭議：若舉證標準過於寬鬆，是否可能導致企業須承擔過度沉重之法律風險與責任？此點應由立



doi:10.6342/NTU202501770

法與實務審慎衡平。

三、舉證困難與專家鑑定

在個資外洩案件中，由於事涉電腦系統架構、網路安全技術及資料庫存取管理等高度專業領域，法院往往需依賴專家鑑定意見來釐清資料外洩的成因與事故鏈條。然而，實務上專家意見可能因所依據之鑑定標準、技術方法或對於事實的理解不同而產生差異，進而導致法院在認定因果關係時面臨困難。

尤有進者，法院是否應受行政機關（如個人資料保護專責機構或主管機關）檢查報告、裁罰決定或調查結果之拘束，亦為實務爭議焦點。臺灣高等法院於 112 年度上字第 656 號民事判決中，即明確表示數發部及交通部觀光局之調查程序與訴訟事件程序不同，且其認定並無拘束民事法院之效力，換言之，即使行政機關曾作出裁罰或認定企業已盡個資法第 27 條所規定適當安全維護措施，法院仍得依其自由心證另為不同判斷。

此判斷結果具一定道理，因行政程序與民事訴訟在程序設計、舉證標準及審查密度上均有所不同。行政裁罰往往以書面資料審查為主，且舉證責任較為寬鬆，重點在於是否違反行政規範；而民事訴訟則強調當事人對於請求權基礎之舉證義務，並需符合高度證明標準。因此，法院主張應保留對證據獨立審酌之權限，以避免行政調查偏誤或程序瑕疵影響民事裁判結果，實有其合理性。

惟從企業實務觀點出發，此一立場亦可能造成法遵風險的不確定。企業如已依行政機關建議改進資安措施，倘若法院仍另為不利於企業之認定，將導致企業對於合規標準無所適從。因此，未來實務運作上，法院應在維持審判獨立原則之餘，對行政調查報告、鑑定意見之內容加以「補充性參酌」，並於判決理由中具體說明其採納與否的依據，以維護法律適用的一致性與預測可能性。

## 第四項 企業安全維護義務與通知補救

一、企業安全措施的審查

根據個資法第 27 條規定，非公務機關保有個人資料者，應採取適當安全措施以防止資料遭不法利用。法院在審查時，會檢視企業是否依據自身業務特性、資源分配及技術發展，建立並落實完善的資料安全管理機制。安全措施包括技術防火



doi:10.6342/NTU202501770

牆、資料加密、入侵偵測、異常存取監控、定期風險評估及內部員工教育等。若企業未能舉證證明其已依法定標準進行防範，則容易被認定存在過失，從而承擔推定過失責任。

二、事故發生後的通知義務與補救措施

除了事前防範，企業在發生資料外洩事件後，亦有法定義務及時通知當事人，並啟動補救機制。法院常會關注企業是否在得知外洩風險後迅速斷開外部連線、加強安全防護，並以適當方式告知受影響之當事人。若企業在事故發生後延誤通知或採取不當措施，不僅加重受害人損害，亦會成為認定其管理疏失的重要依據，從而影響損害賠償金額的裁定。

三、案件事實對賠償計算的影響

具體案件中，法院還會綜合考量個資外洩事件的資料種類、外洩數量、事故後企業採取的補救措施以及第三人介入情形等事實。若認為事故屬於偶發或第三人故意介入導致損害，則企業的賠償責任可能相應減輕；反之，若資料外洩情節嚴重、補救不及時，則可能支持較高額的賠償請求。

## 第五項 損害賠償範圍與計算

一、損害賠償金額認定標準

損害賠償範圍在個資外洩案件中涉及財產上損失與非財產上損害（如精神慰撫金）的雙重考量。根據個資法第 28 條[95]之規定，即使受害人未能證明具體財產損失，亦可請求相當金額的精神慰撫金。法院在具體裁定時，通常會根據事故的侵害情節、受害人所遭受的精神或其他非財產性損害，以及企業違法行為的嚴重性來衡量賠償金額，通常在每人每一事件 500 元以上至 2 萬元以下的範圍內作出裁量。

二、消費者自身責任的影響

除了企業過失外，部分判決亦考量消費者在防範詐騙及資料保護上的自我注意義務。若法院認定消費者因自身疏忽或對詐騙訊息缺乏警覺，導致損害擴大，則

[95] 個資法第 28 條。



doi:10.6342/NTU202501770

可能部分減輕企業應負的賠償責任。這種觀點在判決中常以「消費者自我防衛不力」為理由，對原告賠償請求作出調整，進一步影響最終的賠償金額。

三、案件事實對賠償計算的影響

具體案件中，法院還會綜合考量個資外洩事件的資料種類、外洩數量、事故後企業採取的補救措施以及第三人介入情形等事實。若認為事故屬於偶發或第三人故意介入導致損害，則企業的賠償責任可能相應減輕；反之，若資料外洩情節嚴重、補救不及時，則可能支持較高額的賠償請求。

四、第三人介入與消費者自身責任考量

(一) 第三人介入問題

在多起案件中，法院面臨的主要爭議之一是詐騙集團等第三人的介入是否中斷了企業行為與消費者損害之間的直接因果關係。部分判決認為，若第三人以故意詐騙行為獨立導致消費者損失，則企業不應對該損害負全責；而另一些判決則主張，企業作為資料管理主體，其安全義務不因第三人介入而自動解除，仍須承擔一定賠償責任。因此，如何界定第三人行為與企業過失之間的連結，成為決定判決結果的重要因素。

(二) 消費者自身疏失的評估

除第三人介入外，法院在審理過程中亦會調查消費者在資料外洩後是否有自我防範不足或疏忽行為。例如，若消費者在接獲疑似詐騙訊息時未能保持警覺，或未及時採取必要的防護措施，則可能被認定部分責任，從而在損害賠償中予以扣減。這種評估既體現了對消費者合理注意義務的認可，也在一定程度上平衡了雙方在舉證責任上的不對稱性。



doi:10.6342/NTU202501770

# 第五章　結論與建議

## 第一節　現行困境

從本研究對臺灣法院判決的系統性分析可見，電商平台業者在面對個資外洩事件時，法律環境充滿不確定性。各級法院在認定企業責任、因果關係及損害賠償金額等方面呈現多元判決模式，同時也反映出個資保護法制在實務適用上的多重挑戰。本研究結合歐盟 GDPR 經驗，提出改善我國個資保護法制的具體建議，期能在維護企業經營彈性與保障個人隱私權之間取得平衡。

從企業的視角檢視目前法院針對個人資料外洩案件民事損害賠償責任認定標準，可以發現存在明顯的不一致與模糊性。法院對個人資料外洩案的判決結果分歧，顯示其在過失認定、因果關係界定及損害賠償範圍方面未形成明確一致的判斷標準。特別是在是否採納行政主管機關的認定結果方面，法院往往未能與行政機關達成一致，導致企業在實務操作上面臨雙重標準的困擾。

具體而言，法院在判定企業是否違反「適當安全維護措施」義務時，傾向依據個案情境判斷業者的安全維護措施是否「足夠」或「合理」，然而法律本身卻未提供明確、統一且具體的技術標準。行政機關雖然制定了相關安全維護管理辦法，並提出應採取的各種技術、行政、物理措施，但法院審理時並未一律予以承認或參考，使得企業即使依行政規定進行安全建置，在司法實務中仍可能因法官主觀認定而遭遇賠償責任。

這種法律適用標準的不一致性，導致企業在實際運作中面臨高度的不確定性，增加企業法規遵循上的風險及成本。企業難以根據司法判決的現狀，預測和評估自身在資安投入上的必要性與有效性。尤其是在快速變化的網路科技環境下，業者需要不斷調整和提升資安措施，但若無明確的法律和實務標準指引，便可能陷入無所適從的困境，無法精準地衡量與投資必要的資安資源。

此外，法院也經常未採納行政機關對於安全措施的認定，甚至與主管機關的調查結果產生矛盾，這使得企業即便已經配合行政機關的調查並做出相應改善措施，在面對民事損害賠償訴訟時，仍可能因法院的不同見解而須承擔賠償責任，對企業而言形成了雙重法律風險。



doi:10.6342/NTU202501770

綜合以上所述，法院判決在個資外洩案件中的標準分歧、未採納行政主管機關的認定結果，且法律未明確具體規範適當安全維護措施的技術標準，形成企業法規遵循的實務困境，未來亟需透過司法或立法方式予以改善，以提供企業更明確的法律依據及操作指引，降低企業經營上的法律不確定性與風險。

## 第二節　對電商平台之建議

隨著數位經濟的快速發展，電子商務平台已成為個人資料大量蒐集、處理與利用的主要場域之一，然而近年來多起個資外洩事件顯示，平台業者在個資保護措施、事故應變處理與法律風險管理上仍有諸多待改善之處。根據前述法院實務案例分析及 GDPR 等國際制度觀察，本章提出下列五大面向之建議，供電商平台業者參考，以強化個資保護並降低潛在責任風險。

一、強化資安防護機制與標準化建置

電子商務平台在運營過程中涉及大量個人資料之蒐集與處理，包括用戶的身分資訊、聯絡方式、信用卡號碼、購物紀錄等，皆屬敏感且具潛在商業價值之資料。一旦外洩，不僅導致消費者受害，更可能損及企業信譽與財務。因此，電商平台必須從制度面與技術面雙軌進行資安防護機制之強化。

(一) 首先，建議導入國際資安標準認證制度，如 ISO/IEC 27001 資訊安全管理系統（ISMS）、ISO/IEC 27701 隱私資訊管理系統（PIMS）等，透過風險評估、存取控管、資料加密、異常偵測等內控設計，建立全方位資安治理架構。

(二) 其次，應強化對資料分類與分級管理，針對不同敏感程度的資料（如身分證號、信用卡資訊、醫療紀錄等）設定不同的防護等級與存取限制。例如，重要個資應以 AES 加密演算法儲存，並限制僅特定授權人員可讀取；一般使用紀錄則可視為一般等級，適用較寬鬆之控管。

(三) 再者，建議定期委託第三方進行滲透測試與弱點掃描，發掘系統漏洞，並於每次重要系統升級後進行重新檢測，避免版本升級過程中產生資安漏洞。此外，可導入「零信任架構」（Zero Trust Architecture），使每一筆資料存取行為皆須經過驗證與授權，有效降低內外部駭侵風險。



doi:10.6342/NTU202501770

二、完備事故通報流程與證據保存紀錄

根據法院實務見解，在判斷企業是否盡到「適當安全維護義務」時，常援引事故發生後之應變作為衡量標準。若企業能即時處理、通報與記錄事故，並提出完整佐證資料，將有助於證明其無重大過失，降低責任風險。電商平台應制定事故通報標準作業流程（SOP），包括以下環節：

(一) 事故偵測與初步通報：明訂何種異常行為應即啟動通報機制，並由資安人員在最短時間內研判事態嚴重性。

(二) 內部通報與跨部門協調：資料事故多涉 IT、客服、法務等單位，應設立橫向聯絡機制，確保事故調查與後續因應一致性。

(三) 對主管機關與消費者之通報：依個資法第 12 條及施行細則第 22 條規定，事故如達通報門檻，應於合理期間內向主管機關及當事人說明事故內容、影響範圍、補救措施及風險建議。

(四) 證據保存與紀錄建檔：系統日誌（log）、伺服器活動紀錄、資安設備報告應即時備份並封存，避免事後遭質疑資料滅失或篡改。

(五) 事後檢討與制度精進：事故處理完畢後，應召開內部檢討會議，更新 SOP 內容並加強教育訓練。

透過上述制度化程序，不僅能提升平台應變能力，也利於日後在訴訟或監管調查中證明企業無故意或重大過失。

三、重視消費者救濟與應變支持

個資外洩後，受害者常面臨詐騙、信用損害、心理壓力等問題，而法院在評估企業責任時，也會觀察平台是否積極協助消費者因應及降低損害。故企業應主動建立對應機制，以重建消費者信任並降低訴訟風險。建議措施如下：

(一) 設立專屬客服與通報窗口，協助受害者查詢個資外洩情形、提供報案協助、彙整詐騙樣態等資訊；

(二) 評估提供階段性補償措施，如免費信用監控服務（credit monitoring）、免費更換帳戶、提供法扶轉介資訊等；



doi:10.6342/NTU202501770

(三) 就外洩事故進行溝通聲明，於平台公告事故狀況與應對計畫，展現誠意與透明度，避免訊息落差造成信任危機；

(四) 若證實因資安疏失造成消費者實際損害，可與當事人協商性解決，簽署和解協議以終結爭議。

在法院判決實務中，企業若能積極補救與協商，也有助於在責任認定與賠償額度方面獲得酌減。

四、建立內部個資保護治理架構與人員培訓

企業內部組織的治理制度是個資保護能否落實的關鍵。建議參考 GDPR 制度精神設置資料保護長（DPO），並設立專責資訊安全或個資管理部門，統籌以下事項：

(一) 進行個資生命週期管理：涵蓋蒐集、處理、儲存、傳輸與刪除階段，確保全程符合法令與內部政策；

(二) 定期實施風險評估與合規審查，針對業務流程與資料處理活動進行風險矩陣分析，提出改善建議；

(三) 建立員工教育訓練機制，特別針對客服、資料分析人員等第一線人員，定期施以資安案例演練與防詐意識訓練；

(四) 建立回報與通報機制，確保每一層級皆能發現並回報潛在資安事件。

(五) 此外，內部管理制度應涵蓋第三方廠商（如雲端平台、物流系統、金流合作方）之監督與契約控管，防止委外成為資安漏洞來源。

五、導入法律與保險工具分散風險

在面對多變的資安威脅與高額潛在賠償責任時，企業應以合約與保險兩大工具作為風險轉嫁與緩衝機制。

(一) 在合約面，建議電商平台：

1. 檢視與供應商、第三方處理者、技術平台間的契約條款，明訂資安事件通報義務、賠償責任與監督機制；

2. 加入資安審核與查核條款，確保合作對象具備合理資安防護能力；



doi:10.6342/NTU202501770

3. 對外公布平台個資處理聲明與隱私政策，明確告知消費者其資料使用方式及權利行使管道。

(二) 在保險面，建議企業投保資安責任險（Cyber Liability Insurance）或個資外洩專案保險，以涵蓋以下風險：

1. 因駭客或內部失誤造成個資洩漏之民事損害賠償；

2. 資安事故處理過程之法律費用、鑑識服務、通知成本與品牌復原行銷費用；

3. 營業中斷、商譽受損等間接損失；

4. 若遭主管機關處以罰鍰，部分保單亦可提供行政裁罰補償。

電商平台在數位時代扮演重要資訊中介角色，對個資安全的管理不僅關係消費者權益，更關係企業聲譽與經營永續。惟有主動強化內控機制、建立制度化應變流程、完善風險治理架構，方能在法律責任與商業信任之間取得平衡。隨著我國個資法修法趨嚴與法院判決逐步建立新標準，平台唯有將資安視為核心治理議題，方能於競爭激烈之電商市場中穩健成長，並爭取消費者長期信賴。

## 第三節　對法院與實務運作之建議

近年來，隨著個資外洩事件頻繁發生，法院所面對的民事損害賠償案件日益複雜，不僅涉及高度技術性的資安證據判斷，亦需在資訊不對稱的背景下衡量責任分配與風險歸屬。然觀察我國實務判決可見，法院在舉證門檻設定、外洩來源推定方法、安全維護措施標準之判準上，迄今未能建立穩定一致的裁判架構，導致同類型案件中判決結果顯著歧異，判決說理亦未必清楚揭示審查標準。此種不確定性不僅削弱了消費者尋求救濟之信心與可能性，也使企業難以預測自身法律責任邊界，進而影響資安投資與風險控管策略之制定。

學者提出，現行個資法下，法院對於損害賠償金額的認定，因損害多屬抽象、主觀且難以計算，且安全維護措施標準未有明確規範，導致同類案件賠償數額差異甚大，審判標準亦不明確，進而產生高度的不確定性[96]。亦有學者分析，法院對於

[96] 葉奇鑫、李相臣（2012），〈淺談個人資料保護法民事賠償責任及數位鑑識相關問題〉，司法新



doi:10.6342/NTU202501770

「因果關係認定」未盡相同，舉證責任分配與外洩來源推定方法各異，造成判決結果難以預測，企業與消費者均難以掌握法律風險[97]。

此外，法院在處理個資外洩事件時，需在法律原則與技術事實間尋求平衡，若欠缺明確審查基準與責任認定架構，將導致司法資源重複耗費、企業遵循成本升高，最終損及數位經濟與個資保護制度的發展。學者建議，應建立明確、可預期且符合當代資安治理實況之裁判標準，作為未來案件審理、行政處分評價及企業風險管理之共同依循。為促進個資法之有效運作與數位經濟環境下司法裁判之可預期性，本文建議法院在處理個資外洩損害賠償案件時，應從下列幾方面進行實務標準之強化與制度設計之調整：

一、強化舉證責任轉換與推定機制，落實個資法第 29 條保護目的

在個資外洩損害賠償案件中，舉證責任的分配為訴訟勝敗的關鍵。現行個資法第 29 條雖規定「非公務機關因故意或過失」致資料外洩應負損害賠償責任，學理與實務多認此規定已內含過失推定與舉證責任轉換意旨，惟法院在實際操作上標準不一，有採嚴格證明者，有採寬鬆推定者，致使裁判結果分歧。為提升法律的可預測性與消費者保護效果，建議法院應建立較明確的舉證轉換判準，例如：原告能證明其曾將個資提供予特定被告、所涉詐騙資訊與該企業所蒐集資訊具有高度重疊性、已排除其他可能外洩管道或該企業係唯一可能持有者。此時，應推定該企業為可能外洩來源，由企業負舉證責任證明其已依「當前科技水準與實務可行手段」採行適當安全措施，並無疏失或外洩源於其他因素。此原則亦可參考德國與奧地利法院在適用 GDPR 第 82 條時所發展之「事實推定」原則（Faktischer Anscheinsbeweis），即在資料控制者掌握全部資訊且原告舉證困難時，法院可推定控制者負責，並由其負舉反證責任。

此一制度設計可參考臺灣法院在民法第 191 條之 1 與消費者保護法第 7 條所

---

聲，第 101 期第 3 篇，2012 年 1 月，頁 33-49。

[97] 蔣瑜玲（2023），〈簡析企業個資外洩事件之損害賠償請求－以臺中地方法院 111 年度消字第 3 號民事判決為例〉，科技法律透析，第 35 卷第 1 期，2023 年 1 月 15 日，頁 10-13。



doi:10.6342/NTU202501770

建構之產品瑕疵責任案件中，針對消費者無法取得內部製造流程與技術證據時，法院所發展之「事實推定」、「舉證責任緩和」等認定模式。例如消費者無從掌握製程瑕疵，法院可基於損害發生態樣與產品使用狀況，合理推定為製造商責任。相同邏輯亦可運用於企業掌控資訊環境之個資案件，強化對資訊弱勢之保護。此外，法院亦可引介「醫療過失訴訟」之實務經驗，例如當醫療機構未完整記錄病歷或病患無法釐清診療決策細節時，法院會視為過失推定前提。個資案件中如企業未保存完整系統記錄或資安稽核紀錄，即應合理承擔舉證不利風險。

二、建立可操作之外洩來源推定標準，降低認定分歧

法院在個資外洩案件中面對外洩來源認定的難題時，常陷入過度依賴「技術證據」或企業主張「無異常紀錄」的困境，導致舉證落差過大。實務上，若原告能舉證其個資確實提供予某特定平台，且詐騙內容所揭露資訊為該平台特有資料型態，例如訂房細節、消費紀錄、用餐內容等，法院應以「高度資料重合性」與「唯一資料持有者」為推定外洩來源的條件之一，並視是否有大量同期類似詐騙事件作為佐證，建立具操作性的「事實推定鏈」。

若企業主張其非外洩來源，法院應要求其提出足夠之「排他性證據」，如完整系統存取紀錄、伺服器日誌、防火牆紀錄、外部資安稽核報告等，並說明其資安管理是否符合同業標準與主管機關指引。此外，若企業主張資料外洩係因不可抗力，如 APT 攻擊、零日漏洞或供應鏈資安事件，法院應要求其證明已符合「最大努力原則」（best effort standard），即企業是否依據當時可得資訊與技術資源，已履行合理預防義務。

三、參酌國際標準與政策準則，統一資安義務之審查依據

個資法第 27 條要求非公務機關應採取防止個資洩漏或不當使用之「適當安全措施」，惟目前法院對何謂「適當」缺乏一致性，有法院僅以是否有資安異常通報、有無即時公告警示作為免責依據，有失立法原意。建議法院宜引入「結構性資安管理審查標準」，可從以下五面向評價企業是否已善盡保護義務：

1. 政策與組織面：是否有制定正式資訊安全政策並設有資安負責部門。

2. 技術防護面：是否導入加密、防火牆、存取控管、多因素認證等基本防護。



doi:10.6342/NTU202501770

3. 人員訓練面：是否定期辦理資安訓練與社交工程演練。

4. 稽核與通報面：是否實施定期內部稽核與異常事件即時通報制度。

5. 事後應變與修正面：是否具備資料外洩應變計畫及事後補償與通報機制。

法院亦可參考 ISO/IEC 27001（資訊安全管理系統）與 ISO/IEC 27701（隱私資訊管理系統）等國際標準，以及我國 NCC、數位發展部等機關發布之資安分級要求，作為審查依據，提升企業對裁判預期之可及性。

四、明確法院對行政機關認定之處理原則，促進司法與行政一致性

目前法院對主管機關違規認定是否具證據效力，處理方式不一。建議法院建立三階段原則，以促進司法與行政一致性，避免裁決標準落差，並提升整體制度信賴。

1. 作為初步證據：如主管機關認定企業有具體資安或是個資管理缺失，法院應合理視為初步事實認定依據，企業如欲否認，須提出反證。

2. 若法院見解不同，應說明理由：如因行政認定標準與實務技術發展脫節、調查程序未盡完備等，法院應具體說明其不採之理由。

3. 作為輔助資料參考：即便無具體行政處分，法院亦可參照主管機關調查報告、警示訊息或技術文件，補充其判決說理與證據基礎。

五、建立司法—行政—產業三方對話機制，提升專業判斷與制度整合

資安與個資案件涉及高度技術問題，單靠當事人聲請鑑定與書面資料，法院難以掌握全貌。建議由最高法院、高等法院定期與主管機關（如數位發展部、金管會）及業界、公協會建立對話平台，參考德國 BGH 等法院運作經驗，發佈判決指引、說明舉證標準、資料流向分析模型與合理防護義務範圍。法院亦可與第三方資安鑑識機構建立合作，研議一致性審查指標，協助裁判中落實風險導向思維與科技事實評價。

綜上所述，法院於個資外洩案件中若能建立明確一致之認定架構，不僅可提升裁判之信賴與正當性，更有助企業理解法律風險邊界，合理配置資安資源，並引導企業合規治理與預防措施之制度化發展。



doi:10.6342/NTU202501770

## 第四節　對法律修正之建議

近年來，電子商務快速發展所引發的個資保護問題，逐漸暴露出我國個資法在規範架構與實務運作上的諸多缺漏。透過對國內法院判決實務的分析，以及與歐盟 GDPR 之制度比較可知，我國法制在個資外洩事件的民事責任認定、主管機關功能、罰則設計與預防機制等層面，亟需進行系統性修正。為建立更具預測性與實效性的個資保護法制，本文提出下列數項修正建議，供立法機關與主管機關參考：

一、建立「明確化」的適當安全維護標準，提高業者可預期性

我國個資法第 27 條雖已要求非公務機關採取「適當之安全維護措施」，惟該條規定抽象，未具體指明技術與管理上的最低標準，導致法院在判斷企業是否盡責時標準不一，增加企業合規不確定性與司法資源耗費。因此，建議修法時應授權主管機關（即未來之個人資料保護委員會）訂定具體且可操作之「資安責任準則」或「業別指引」，例如：參考 GDPR 第 32 條[98]所列「技術與組織措施」類型，如加密、假名化、風險評估制度、資安事件日誌保存等；對電商、金融、醫療等不同類型產業訂定分級資安防護準則；每年公告「最低資安基線」，供企業參考並據以設計資安架構；要求高風險資料處理者進行年度外部資安稽核或資安鑑定。透過上述指引與制度化準則，法院得以有一可參酌的審查基準，企業亦可提高遵法明確性，強化風險自主管理能力。

二、引進資料保護影響評估與資料保護長制度，強化預防式治理機制

根據歐盟 GDPR 第 35 條[99]規定，企業如涉及大量敏感個資處理、高風險科技應用或自動化決策，應進行「資料保護影響評估」（DPIA），以預先評估風險並制定減輕措施；此外，GDPR 第 37 條亦要求企業指派資料保護官（DPO），作為內部監督與對外溝通之窗口。我國雖於 2023 年修法草案中提出設置「個資保護長」，但未具強制性、未涵蓋非公務機關，亦未建立完整的風險預防制度。建議我國應仿照 GDPR 制度，明定如下修法方向：強制大型電商或處理大量個資之業者設置「個資

---

98 General Data Protection Regulation, Art.32.

99 General Data Protection Regulation, Art.35.



doi:10.6342/NTU202501770

保護長」，負責制度建置、稽核、教育訓練與通報程序；增訂 DPIA 制度，對涉及大規模個資蒐集或敏感資料處理之行為，要求預作風險評估報告，並提交主管機關備查；規範「隱私權預設」（Privacy by Design and by Default）原則，要求系統設計即納入資料最少化與風險控管思維。透過此預防性機制，可大幅降低資料外洩事件發生機率，亦提升企業治理水準與社會信任基礎。

三、強化個資事故通報義務，保障消費者即時反應權益

目前個資法對資料外洩通報義務雖有規範，惟缺乏具體程序與罰則，實務上企業延遲通報、通知內容含糊不清之情形屢見不鮮。此不僅阻礙主管機關掌握資訊，亦妨害消費者採取必要防範行動。建議明定以下制度：

(一) 參考 GDPR 第 33 條，資料外洩應於 72 小時內通報主管機關，並說明：外洩類型與影響範圍、涉及資料項目類型、已採取或計畫採取之補救措施。

(二) 若外洩可能對當事人權益造成重大影響，應同時通知當事人，並清楚說明風險與自救建議，例如：預警詐騙手法（如解除分期付款）、提供信用監控工具或法律諮詢窗口、明示資料被盜用時之申訴與求償流程。

(三) 訂定未通報或故意延遲之行政罰鍰，確保制度具有效性與強制力。

四、補強民事損害賠償制度，明定損害類型與因果關係舉證準則

我國個資法第 29 條雖設有推定過失制度，但在法院實務中，仍常以「無法證明外洩源頭」「詐騙與外洩無相當因果關係」為由駁回請求，使受害人處於高度不利地位。建議可從以下面向補正：

(一) 明確損害類型範疇：明文化學理上已被承認之非財產上損害，例如恐懼、焦慮、隱私喪失、社交名譽受損等；參考 GDPR 第 82 條，採「廣義損害」概念，降低請求門檻；引入「最低損害補償額」制度，對於無法明確量化之損害予以定額補償。

(二) 調整因果關係認定標準：採用「高度相似性」原則，如消費者資料與詐騙集團使用之資料高度一致，推定其來源具相當因果；舉證責任調整為「可得性證明」（access-based burden shifting），若平台掌控資料來源且不提供資料比對，應負推定責任。賦予主管機關鑑定機能或技術調查權，建立專責「個資鑑定機構」



doi:10.6342/NTU202501770

或協力鑑定機制，以減輕消費者單方舉證困難。

五、健全主管機關功能，落實獨立監理與跨部會協調機制

目前個資法雖已修法設立「個人資料保護委員會」，惟制度尚在推動初期，未來能否發揮有效監督與政策引導功能，仍仰賴法規設計與實務運作完善。建議應：

(一) 確保個資會具備「實質獨立性」、預算自主與跨部會協調權；

(二) 賦予個資會統一標準訂定、行政指導、檢查查核與行政處分等完整權限；

(三) 建置與公務機關之協調平台，破除目前部會分屬之執法斷裂；

(四) 授權個資會針對不同業別訂定資安基準、公告風險等級。

透過制度性獨立與功能性專業之結合，有助我國邁向更現代化、可治理與可信賴的個資保護體系。

我國個資法面對高度數位化的電商社會，必須從保障消費者資訊自主權與提升企業合規預見性雙面出發，推動整體制度之轉型升級。本文建議修法方向，從明確安全標準、建立預防性治理、強化通報制度、補正民事責任認定、導入懲罰性機制至健全監理結構，期能構築一個能有效回應資安挑戰、平衡產業發展與權益保護的現代法律體系。



doi:10.6342/NTU202501770

# 參考文獻

【中文文獻】（依作者姓氏筆畫順序排列）

一、中文書籍

1. 江雅綺，數位平台經濟的法律挑戰，漢蘆圖書出版有限公司，初版（2021）。
2. 李震山，人性尊嚴與人權保障，元照出版有限公司，2009 年。
3. 林洲富，個人資料保護法之理論與實務，元照出版有限公司，修訂二版（2019）。
4. 劉佐國/李世德，個人資料保護法釋義與實務，碁峯資訊，2012 年 8 月（二）期刊部份。

二、期刊文獻

1. 王德瀛（2020），〈簡評加州消費者隱私保護法－規範重點與其對美國隱私保護的影響〉，科技法律透析，第 32 卷第 3 期，頁 19-27。
2. 尤重道（2017），〈個人資料保護之概念與蒐集處理利用暨違法責任（上）〉，全國律師，21 卷 7 期，頁 85-94。
3. 尤重道（2017），〈個人資料保護之概念與蒐集處理利用暨違法責任（下）〉，全國律師，21 卷 8 期，頁 71-89。
4. 李世德（2018），〈GDPR 與我國個人資料保護法之比較分析〉，臺灣經濟論衡，16 卷 3 期，頁 69-93。
5. 李億誠（2019），〈歐盟一般資料保護規則（GDPR）裁罰案例解析〉，科技法律透析，31 卷 12 期，頁 26-38。
6. 李相臣、葉奇鑫（2012），〈淺談個人資料保護法民事賠償責任及數位鑑識相關問題〉，司法新聲，第 101 期第 3 篇，頁 33-49。
7. 余俊賢（2010），〈因應個資法修正後電子商務業者之資料安全管理與稽核實務〉，電腦稽核，第 22 期，頁 103-109。



doi:10.6342/NTU202501770

8. 張志偉（2020），〈歐盟資料保護基本規則之適用範圍〉，臺灣科技法學叢刊，創刊號，頁 129-164。

9. 張陳弘（2022），〈美國加州消費者隱私保護法制之最新發展與比較法啟示〉，當代法律，第 6 期，頁 24-39。

10. 張陳弘（2024），〈企業蒐用消費者資料之個資保護法制思維－美國加州消費者隱私法之借鏡〉，中正大學法學集刊，第 85 期，頁 57-129。

11. 黃小玲（2011），〈個資法與國際隱私管理標準、規範之分析與應用〉，資訊安全通訊，17 卷 3 期，頁 22-36。

12. 楊政一（2023），〈個資事故的「損害」是什麼？以德國近期法院民事判決為例〉，科技法律透析 35 卷 1 期，頁 38-43。

13. 楊政一（2023），〈歐盟 GDPR 框架下德國民事個資侵權體系對我國之啟發〉，科技法律透析，第 35 卷第 6 期，頁 31-50。

14. 曾更瑩（2013），〈企業因應個資法面臨的難題〉，全國律師，2013 年 4 月，頁 5-14。

15. 廖淑君（2019），〈論我國因應 GDPR 施行之措施－以個人資料之跨境傳輸為核心議題〉，商業法律與財金期刊，第 3 卷第 1 期，頁 115-140。

16. 蔣瑜玲（2023），〈簡析企業個資外洩事件之損害賠償請求－以臺中地方法院 111 年度消字第 3 號民事判決為例〉，科技法律透析，第 35 卷第 1 期，頁 10-13。

17. 蔡宜臻（2023），〈美國聯邦資料隱私和保護法案介紹〉，科技法律透析，第 35 卷第 7 期，頁 30-37。

18. 蔡朝安（2013），〈個人資料保護實務：以遵法及風險管理為中心〉，資訊安全通訊，19 卷 3 期，頁 80-95。

19. 蔡柏毅（2021），〈有過必悛－違反個資法的責任與罰則〉，財團法人金融聯合徵信中心－法規時論，頁 52-62。



doi:10.6342/NTU202501770

20. 董漢忠（2020），〈歐盟個資法（GDPR）帶來的省思－如何將個資保護精神整合入網站設計原理之探討〉，證券服務，第 676 期，頁 21-40。

三、臺灣臺灣學術論文

1. 方俊明（2023），個資法民刑事責任研究，東吳大學法律學系碩士論文。
2. 林秉輝（2022），企業洩漏個人資料之責任－以 GDPR 為中心，中原大學財經法律學系碩士論文。
3. 涂詩娥（2013），個人資料保護法委外監督與責任之研究－以資訊服務業為中心，東吳大學法律學系碩士論文。
4. 張夢麒（2012），個資法施行後企業風險之具體趨避模式－以委外企業為例，東吳大學法律學系研究所碩士論文。
5. 張容涵（2019），從比較法觀點探討我國個資保護制度之轉型，國立臺灣大學法律學系碩士論文。
6. 詹婉琬（2020），以 ISO 27701 隱私資訊管理系統為核心探討對我國個人資料保護法之影響，國防大學資訊管理學院資訊管理學系碩士論文。
7. 陳惠宣（2021），電子支付與個人資料保護法之研究－以 GDPR 為中心，世新大學法律學研究所碩士論文。
8. 廖珮雲（2018），企業大數據與個人資料保護法之研究－以金融業為中心，東吳大學法律學系碩士論文。
9. 謝乃文（2013），論企業委外業務個人資料保護之風險－以汽車租賃業為例，東吳大學法律學系碩士論文。
10. 蔣哲宇（2019），個人資料保護法下對電商業適當安全維護措施之行政檢查，東吳大學法律學系科技法律研究組碩士論文。
11. 羅一倫（2012），論個人資料保護法對產業之影響與因應，東吳大學法律學系研究所碩士論文。
12. 蘇峻毅（2022），論非公務機關違反個人資料保護法上義務之損害賠償責任，東海大學法律學系研究所碩士論文。



doi:10.6342/NTU202501770

四、本文選錄之裁判


1. 臺灣士林地方法院 107 年度湖小字第 401 號民事判決（107 年 6 月 15 日）。
2. 臺灣士林地方法院 108 年度湖小字第 558 號民事判決（108 年 6 月 3 日）。
3. 臺灣士林地方法院 107 年度消字第 6 號民事判決（108 年 10 月 31 日）。
4. 臺灣臺中地方法院臺中簡易庭 110 年度中簡字第 1952 號民事判決（111 年 12 月 23 日）。
5. 臺灣臺北地方法院 111 年度北簡字第 1007 號民事判決（111 年 3 月 24 日）。
6. 臺灣臺北地方法院 111 年度簡上字第 266 號民事判決（112 年 5 月 17 日）。
7. 臺灣臺北地方法院 111 年度訴字第 5578 號民事判決（112 年 3 月 20 日）。
8. 臺灣新竹地方法院 111 年度竹東簡字第 48 號民事判決（112 年 9 月 22 日。
9. 臺灣臺中地方法院 111 年度訴字第 2708 號民事判決（112 年 3 月 15 日）。
10. 臺灣臺北地方法院 111 年度北簡字第 16345 號民事判決（113 年 3 月 19 日）。
11. 臺灣臺北地方法院 112 年度訴字第 3711 號民事判決（112 年 12 月 8 日）。
12. 臺灣臺中地方法院 112 年度簡上字第 120 號民事判決（112 年 12 月 15 日）。
13. 臺灣新北地方法院三重簡易庭 112 年度重小字第 3188 號民事判決（112 年 11 月 21 日）。
14. 臺灣臺北地方法院 112 年度訴字第 2854 號民事判決（113 年 4 月 12 日）。
15. 臺灣新竹地方法院 112 年度簡上字第 143 號民事判決（113 年 6 月 26 日）。
16. 臺灣高等法院 112 年度上字第 656 號民事判決（113 年 1 月 30 日）。
17. 臺灣高等法院臺中分院 112 年度上易字第 208 號民事判決（113 年 5 月 17 日）。
18. 臺灣高等法院 113 年度上易字第 471 號民事判決（113 年 10 月 22 日）。


五、（網路文獻）（依作者發表年份排序）


1. 數位時代〈微風個資外洩，經濟部、數發部組調查小組要查！誰讓 90 萬會員個資曝風險？〉，https://www.bnext.com.tw/article/74218/breeze-mall-hack?




doi:10.6342/NTU202501770

2. 經濟部〈經濟部對微風集團發生個資外洩事件之調查說明〉，https://www.moea.gov.tw/MNS/populace/news/News.aspx?kind=1&menu_id=40&news_id=105735
3. 今周刊〈和泰旗下 iRent 爆個資外洩，公司道歉了…14 萬用戶擴大認定 40 萬，賠償方案「這天」出爐〉，https://www.businesstoday.com.tw/article/category/183027/post/202302020015/
4. 內政部警政署刑事警察局〈公布 113 年第四季高風險業者排名 提醒消費者慎防詐騙〉，https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1887&serno=99151900-b8cb-4b95-bc5c-f3b0e8b51f94
5. iThome（2021 年 7 月 30 日），〈亞馬遜違反 GDPR 被罰 7.46 億歐元，創史上最高金額〉，載於：https://www.ithome.com.tw/news/145975（最後瀏覽日：2025 年 5 月 1 日）。
6. iThome（2019 年 1 月 22 日），〈Google 違反 GDPR 被法國重罰 5,000 萬歐元〉，載於：https://www.ithome.com.tw/news/128391（最後瀏覽日：2025 年 5 月 1 日）。
7. 「立法院三讀通過個資法修正案 將強化企業個資外洩罰責 並盡速設置個資保護委員會籌備處」，國家發展委員會，網址：https://www.ndc.gov.tw/News_Content.aspx?n=114AAE178CD95D4C&s=4CE6D4554ACDEF7E
8. 「政院通過『個人資料保護法』第 1 條之 1、第 48 條、第 56 條修正草案 設置個資保護獨立監督機關並提高個資外洩罰責」，行政院全球資訊網，2023 年 4 月 13 日，網址：https://www.ey.gov.tw/Page/9277F759E41CCD91/2d6bb590-fa47-435f-818e-c196c25733e0
9. 「取得政府機關或第三方公正單位的認證，是否就能免於個資賠償責任?」中華數位企業資料保護專區，2024 年 11 月 14 日，網址：https://www.softnext.com.tw/dataprotection/rule_d04.html



doi:10.6342/NTU202501770

【英文文獻】（依作者姓氏英文字母順序排列）


1. activeMind.legal （2025）, When Does the GDPR Apply to Non-EU Businesses?, in: https://www.activemind.legal/guides/gdpr-non-eu-businesses/ （最後瀏覽日：04/07/2025）
2. Arthur Cox （2024）, Summary of 2023’s Key CJEU Data Protection Judgments, in: https://www.arthurcox.com/knowledge/summary-of-2023s-key-cjeu-data-protection-judgments/ （最後瀏覽日：05/25/2025）
3. Arthur Cox （2025）, Summary of 2024’s Key CJEU Data Protection Judgments, in: https://www.arthurcox.com/knowledge/summary-of-2024s-key-cjeu-data-protection-judgments/ （最後瀏覽日：05/29/2025）
4. Clyde & Co （2024）, The New Leading Decision Procedure of the Federal Court of Justice on Damages under the GDPR, in: https://www.clydeco.com/en/insights/2024/11/the-new-leading-decision-procedure-of-the-federal （最後瀏覽日：05/25/2025）
5. Clyde & Co （2025）, Loss of control over personal data: Is that sufficient for GDPR compensation?, in: https://www.clydeco.com/en/insights/2025/02/loss-of-control-over-personal-data （最後瀏覽日：05/25/2025）
6. Consilium （Council of the European Union） （2025）, General Data Protection Regulation （GDPR）, in: https://www.consilium.europa.eu/en/policies/data-protection-regulation/ （最後瀏覽日：04/07/2025）
7. Covington & Burling LLP （2023）, CJEU Clarifies the GDPR’s Right to Compensation, in: https://www.insideprivacy.com/eu-data-protection/cjue-clarifies-the-gdprs-right-to-compensation/ （最後瀏覽日：05/25/2025）
8. DLA Piper Privacy Matters （2024）, EU CJEU Insight: Key Takeaways from Recent Rulings on GDPR Damages, in: https://privacymatters.dlapiper.com/2024/10/eu-cjeu-insight/ （最後瀏覽日：05/29/2025）




doi:10.6342/NTU202501770

9. DLA Piper Privacy Matters （2024）, Germany: Judgment on Non-Material Damages for Loss of Control over Personal Data, in: https://privacymatters.dlapiper.com/2024/11/germany-judgment-on-non-material-damages-for-loss-of-control-over-personal-data/ （最後瀏覽日：05/29/2025）
10. EUR-Lex （2018）, General Data Protection Regulation （GDPR） applies from 25 May 2018, in: https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html （最後瀏覽日：04/07/2025）
11. GDPRhub （2024）, CJEU – C-300/21 – Österreichische Post （Non-material damage in connection with the processing of personal data）, in: https://gdprhub.eu/index.php?title=CJEU_-_C-300%2F21_-_%C3%96sterreichische_Post_%28Non-material_damage_in_connection_with_the_processing_of_personal_data%29 （最後瀏覽日：05/25/2025）
12. GDPRhub （2024）, CJEU – C-667/21 – Krankenversicherung Nordrhein, in: https://gdprhub.eu/index.php?title=CJEU_-_C-667%2F21_-_Krankenversicherung_Nordrhein （最後瀏覽日：05/25/2025）
13. GDPRhub （2024）, CJEU – C 456/22 – Gemeinde Ummendorf, in: https://gdprhub.eu/index.php?title=CJEU_-_C%E2%80%91456%2F22_-_Gemeinde_Ummendorf （最後瀏覽日：05/25/2025）
14. GDPRhub （2024）, C 182/22 and C 189/22 – Scalable Capital （Joined Cases）, in: https://gdprhub.eu/index.php?title=CJEU_-_C%E2%80%91182%2F22_and_C%E2%80%91189%2F22-Scalable_Capital%28Joined_Cases%29 （最後瀏覽日：05/29/2025）
15. GDPRhub （2024）, BGH – VI ZR 10/24, in: https://gdprhub.eu/index.php?title=BGH_-_VI_ZR_10%2F24 （最後瀏覽日：05/29/2025）
16. Harneys （2024）, CJEU Ruling Clarifies on Liability, Damages and TOMs for Data Breaches, in: https://www.harneys.com/our-blogs/regulatory/cjeu-ruling-



doi:10.6342/NTU202501770

clarifies-on-liability-damages-and-toms-for-data-breaches/ （最後瀏覽日：05/29/2025）

17. Heinzke, Philippe; Matthiesen, Reemt; Dreyer, Julia （2024）, News from the CJEU on GDPR Compensation, in: https://cms-lawnow.com/en/ealerts/2024/01/news-from-the-cjeu-on-gdpr-compensation （最後瀏覽日：05/29/2025）

18. IBM （2025）, What Is CCPA?, in: https://www.ibm.com/think/topics/ccpa-compliance （最後瀏覽日：04/07/2025）

19. Loyens & Loeff （2023）, Legal Framework on Non-Material Damages under the GDPR: A Status Quo, in: https://www.loyensloeff.com/insights/news--events/news/legal-framework-on-non-material-damages-under-the-gdpr-a-status-quo/ （最後瀏覽日：05/25/2025）

20. Matheson （2023）, CJEU provides clarity on right to compensation for GDPR infringements, in: https://www.matheson.com/insights/detail/cjeu-provides-clarity-on-right-to-compensation-for-gdpr-infringements （最後瀏覽日：05/25/2025）

21. Palo Alto Networks （2025）, What Is the California Consumer Privacy Act （CCPA）?, in: https://www.paloaltonetworks.com/cyberpedia/ccpa （最後瀏覽日：04/07/2025）

22. Secure Privacy （2023）, Protecting Your Personal Data: A Guide to China’s Personal Information Protection Law （PIPL）, in: https://secureprivacy.ai/blog/china-pipl-personal-information-protection-law （最後瀏覽日：04/07/2025）

23. TechTarget （2024）, General Data Protection Regulation （GDPR）, in: https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR （最後瀏覽日：04/07/2025）

24. Timelex （2024）, Recent CJEU Judgements Concerning the Right to Compensation under Art. 82 GDPR: State of Affairs in Ten Focus Points, in: https://www.timelex.eu/en/blog/recent-cjeu-judgements-concerning-right-



doi:10.6342/NTU202501770

compensation-under-art-82-gdpr-state-affairs-ten-focus （最後瀏覽日：05/29/2025）

25. CJEU （2023）, Judgment of 14 December 2023 – Case C-340/21, VB v. Natsionalna agentsia za prihodite （ECLI:EU:C:2023:986）, in: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A62021CJ0340 （最後瀏覽日：05/25/2025）

26. CJEU （2023）, Judgment of 14 December 2023 – C-456/22, in: https://curia.europa.eu/juris/document/document.jsf?text=&docid=290709 （最後瀏覽日：05/29/2025）



doi:10.6342/NTU202501770