臺北高等行政法院判決

高等行政訴訟庭第一庭
112年度訴字第889號
113年12月26日辯論終結

原　　告　旋轉拍賣有限公司

代　表　人　陳翊偉 Marcus Tan Yi Wei（董事）

訴訟代理人　吳志光　律師
　　蕭秀玲　律師
　　黃耀賞　律師
複 代理 人　陳毓芬　律師
被　　告　數位發展部數位產業署

代　表　人　林俊秀（署長）

訴訟代理人　黃國源
　　陳智明

上列當事人間個人資料保護法事件，原告不服數位發展部中華民國112年5月26日數位訴決字第1120004449號訴願決定、112年5月30日數位訴決字第1120005038號訴願決定，提起行政訴訟，本院判決如下：

主　文

原告之訴駁回。

訴訟費用由原告負擔。

事實及理由

一、程序事項：

㈠本件原告起訴後，被告代表人由呂正華變更為林俊秀，茲據現任代表人具狀聲明承受訴訟（本院卷二第357頁），核無不合，應予准許。

㈡行政訴訟法第111條第1項、第2項規定：「（第1項）訴狀送達後，原告不得將原訴變更或追加他訴。但經被告同意或行政法院認為適當者，不在此限。（第2項）被告於訴之變更或追加無異議，而為本案之言詞辯論者，視為同意變更或追加。」查原告起訴時，聲明係為「訴願決定及原處分均撤銷。」嗣因原處分已執行完畢而無回復原狀可能，故變更其訴之聲明為「確認原處分為違法。」（本院卷二第316頁）被告就原告訴之變更並不爭執，故上述原告訴之變更應予准許，合先敘明。

二、事實概要：

緣內政部警政署(下稱警政署)165反詐騙諮詢專線（下稱165專線）依據民眾通報，認原告所經營之旋轉拍賣網路平台，疑似有違反個人資料保護法(下稱個資法)情形，警政署乃先後於民國111年9月 13日、同年10月26日及同年11月30日發函通知被告依權責處理。被告遂依警政署通報，於111年10月24日、同年11月11日函請原告就前開疑似有違反個資法情形，查明妥處，其中併請原告說明就前開事故是否查明後以適當方式通知當事人(即會員、消費者等)，則原告於同年11月8日、同年12月2日函復略以其資訊系統查無遭駭客入侵或有個資被竊取、洩漏、竄改或其他侵害之情形，並無個資法第12條規定應通知當事人情形。嗣被告於111年12月30日召開個人資料保護行政檢查會議(下稱行政檢查會議)，並通知原告出席會議說明，評核結果認為原告就個資外洩情形，未踐行個資法第12條、第27條第1項規定，以適當方式通知當事人及採行適當之安全措施，被告乃先後依同法第48條第2款、第4款規定，於112年1月19日以產經字第1124000044號函（下稱原處分1）、112年2月4日以產經字第11240000661號函（下稱原處分2，並與原處分1合稱為原處分），均限期原告於文到之次日起2個月內改正，並將改正結果逕復被告。原告不服，分別提起訴願均駁回，乃再向本院提起本件行政訴訟。

三、本件原告主張：

㈠個資法第12條規定之個資外洩事故通知，限於資料控管者持有之個人資料在當事人不知情之情況下遭到侵害，因此責成資料控管者盡速通知當事人，使受到個資侵害事故影響之當事人採取防範措施和提高警覺，以防止駭客利用不法取得之個人資料進行詐騙。個資法第12條規定不應濫用於網路釣魚詐騙案件。蓋165專線提供原告通報資料的頻率為每星期1次，且因遮蔽可辨識被害人和加害人之個人資料，致原告無法辨識多數已受害的當事人身分。原告如依被告要求每星期頻繁通知所有可能受侵害之當事人（亦即全體用戶），將造成狼來了效應遞減。一旦真的收到個人資料外洩通知，當事人警覺性恐已麻痺。另封鎖用戶於對話功能傳送QR Code或外部網站連結，不應視為個資法第27條第1項規定對於個人資料檔案採行之適當安全措施。傳送QR Code或外部網站連結，本來是民眾使用網路常見之溝通方式（包括司法院、警政署和其他主管機關亦提供民眾與其聯繫之Line連結）。原告願意配合政府打詐，但被告不應任由詐騙集團消遙法外持續透過網路釣魚話術詐騙民眾，即怪罪原告對於保有之個人資料檔案沒有採行適當安全措施。實則，原告於112年2月7日收到原處分2前，已採取下列警示和封鎖措施：1.用戶於對話功能傳送QR Code，系統自動跳出警示訊息；用戶點擊外部網站連結，將被系統自動導向警示頁面（111年7月起）；2.用戶於對話功能傳送手機號碼或電子信箱地址，系統自動跳出警示訊息（111年9月起）；3.用戶創設帳號後未上架商品即於短時間內傳送QR Code，將被系統自動停權（111年12月起）；4.全面禁止用戶於對話功能傳送外部網站連結和電子郵件信箱（112年1月起）。惟實施上述阻斷QR Code及惡意連結之措施後，仍無法追趕日新月異之詐騙手法。詐騙集團發現QR Code和外部網站連結遭封鎖後，即不斷變更文字與數字的不同組合，創設各種變形符號，突破原告不斷重新設定之關鍵字封鎖，目的都在誘使網路賣家輸入詐編

集團的Line 後加入Line好友，再於原告無法控制之Line聊天室假冒客服和銀行人員進行詐騙。被告除了督促原告進行防詐宣導外，本身也應該正確教育民眾認識網路釣魚詐騙和業者個資外洩之差異，而不是每次接到165專線移送通報案件後，即大張旗鼓檢查原告是否依個資法第27條第1項規定採取適當安全措施，一年多來反覆要求原告填寫「資安訪視紀錄表」、「涉及違規事項--業者意見陳述表」等內容大同小異但內容不盡然適用於原告之表單，罔顧業者商業模式和歹徒詐騙模式之特性，逕將網路釣魚詐騙案件當作原告發生個資外洩事件處理，對外宣揚其已嚴正要求業者重視資安。此種不對外界澄清個資外洩與網路釣魚詐騙差異之政績宣揚，實無助於正確教育民眾明辨網路釣魚詐騙和業者個資外洩所應採取之自我保護措施，亦傷害了因網路詐騙猖獗而同樣深受其害，但持續配合政府打詐以保護消費者之原告信譽。

㈡個資法第12條個資外洩通知義務：

1.個資法第30條第2項及第4項規定，主管機關實施檢查後，應作成紀錄。紀錄於事後作成者，應送達被檢查者，並告知得於一定期限內陳述意見。被告迄今未提供111年12月30日行政檢查會議紀錄，逕以原處分1命當事人踐行個資法第12條之告知義務，顯屬違法。

2.訴願決定1引用法務部106年6月5日法律字第00000000000號函可知個資法第12條適用有下列前提：⑴發生洩漏情事，⑵當事人無法得知，⑶資料控管者應盡速將查明之事實通知當事人。又引用國發會發法字第0000000000號函釋亦說明個資法第12條之通知義務，以「個資有外洩情事」為前提。上開函釋的網路賣家不是被害人，而是可能洩漏個資之資料蒐集者，在此情況下，被竊取的買家個人資料可能來自平台業者或賣家，買家無法得知自己的個人資料已遭到洩漏，因此國發會認為平台業者和賣家均有迅速通知買家之義務。此與網路釣魚詐騙案件係由詐騙集團「直

接」向當事人騙取個資，而非「間接」自當事人以外之其他管道取得，顯有不同。故個資法第12條個資外洩通知義務不適用於網路釣魚詐騙案件。

3.訴願決定1另指出：原告未提出資安鑑識報告、電腦弱點掃描報告等資料佐證，自難採信無平台用戶個資受侵害。查被告於作成原處分1之前，從未要求原告提出上述文件。原告於112年5月26日訴願決定1作成前，已提出以下資料給被告，被告和訴願機關罔顧原告提出之資料，執意認為無法採信無平台用戶個資受侵害，令人遺憾：原告於行政檢查會議前，於「涉及違規事項--業者意見陳述表」說明原告採取之資安防護措施包括：⑴採用Cloudflare Web Application Firewall(Web應用程式防火牆，WAF)過濾及監控HTTP流量保護網路應用程式，防護原告網站及APP免於DoS及DDoS攻擊；⑵透過內部監控工具監控流量，一旦發現異常流量，立即使用Cloudflare防火牆規則封鎖相關IP位址；（3)設置Static Analysis Scanner(靜態分析掃描器）掃描Pull Requests(拉取需求）及防止個人資料外洩；⑷由原告安全團隊人工檢視所有應用程式，每年就對外應用程式執行滲透測試。又原告於112年5月22日回函，提供第三方獨立機構於112年2月7日就旋轉拍賣網站和手機應用程式出具之最新滲透測試報告。另資安鑑識報告係為調查數位證據，資料控管者不得僅因沒有提出此報告即被認定有個資外洩。至於原告提出之滲透測試報告，與被告指摘原告沒有提出之電腦弱點掃描報告，均與偵測系統安全有關，但原告執行之滲透測試周延性更佳。

㈢個資法第27條第1項個人資料檔案之安全措施：

1.原處分2命原告阻斷QR Code或惡意連結，係要求原告藉由全面禁止所有用戶使用QR Code和外部網站連結溝通，以便封鎖可能隱身於正常用戶間之假買家將網路賣家導向Line聊天室，進行假客服和假銀行人員之詐騙，此乃防詐騙措施，但不應被認為是個資法第27條第1項(個資法施行細

則第12條第2項）規定為防止非公務機關「保有」個人資料檔案「被」竊取、竄改、毀損、滅失或洩漏之安全措施。否則，豈非任何容許使用者傳送QR Code或網站連結之網站，均違反個資法第27條應採行適當安全措施之義務？或豈非傳送QR Code或網站連結之使用者，均在破壞網路平台經營者為保護個人資料檔案採取之安全措施？

2. 又如果阻斷QR Code或外部網站連結是非公務機關於個資法第27條第1項規定之義務，被告將此義務僅加諸被告限期改正，否則處以罰鍰，即係對被告為差別待遇，違反行政程序法第6條規定之平等原則。再者，如果不區分防詐騙措施和防止個人資料檔案被侵害之安全維護措施，則被告於個資法第48條修正後，隨時可因原告沒有採行特定之防詐騙措施，無須先命原告改正，即得對原告立即課予罰鍰處分，將傷害原告權益至鉅。

3. 被告命原告阻斷QR Code和網站連結（手段），係為防止網路賣家受到假買家詐騙（目的）。但封鎖QR Code和外部網站連結只是防詐騙措施之一部分，不能全面防詐。原告初期於用戶點選QR Code和外部網站連結時即以彈跳視窗立即警示用戶，繼而禁止用戶傳送QR Code和外部網站連結，但詐騙集團隨即改用文字、數字和各種變形符號之組合，誘拐網路賣家自行輸入詐騙集團的LineID後前往Line聊天室，繼續變身為假客戶和假銀行人員進行詐騙，顯然被告命原告阻斷QR Code和網站連結之手段無助於目的之達成。實則，行政行為態樣很多。被告為實現一定之行政目的，以輔導、協助、勸告、建議或其他不具法律上強制力之方法，促請原告為一定作為或不作為之行為，亦可施以行政指導。原告願意配合政府施政，共同保護消費者，且在被告成立之前，即已自主採取防詐騙措施，並因應詐騙集團手法翻新而對網站上之防詐騙措施採取滾動式之管理，亦願意與被告和刑事警察局交流，以協助主管機關實現防詐騙之行政目的。然被告卻以原告違反個資法第

27條第1項規定之安全措施為由，做成行政處分命原告限期改正，使被告面臨如何遵守個資法規定產生極大疑慮等語，並聲明求為判決：①確認原處分為違法。②訴訟費用由被告負擔。

四、被告則以：

㈠警政署165專線資料庫之紀錄，就民眾通報原告詐騙電話被害案件（下稱系爭通報案件），其內容涉及交易個資等，顯有個資外洩之嫌，原告應盡個資法第12條個資事故通知義務，原告逕認系爭通報案件均為網路釣魚詐騙案件，不負前開義務，洵無可採：

1.被告自111年8月27日成立以來迄同年12月30日止，接獲警政署通報計3次來函，依警政署函所載，其接獲民眾通報原告平台詐騙電話案件，而自111年9月至12月間，每月通報數量分別高達309筆、262筆、616筆及429筆，細觀系爭通報案件內容，其中包含買家因曾經於原告賣場購物，爾後收到詐騙集團電話，以訂單錯誤等內容，引導買家進行ATM相關匯款操作之情形，尤其，詐騙集團向買家提供之資訊，包含購買時間、商品名稱、金額、付款方式等交易資訊，依一般常理可言，非屬一般人可自由得知者，理當可推測係該等交易個資係由原告外洩，故系爭通報案件非純屬網路釣魚詐騙案件，原告反覆強調網路釣魚詐騙與個資外洩之差異，並主張其已就被告機關所提出應釐清案件逐一說明，系爭通報案件所涉均為當事人主動提供個資之網路釣魚詐騙案件，不應與個資外洩案件混淆云云，不足可採。

2.次查，訴願決定1所引用之106年6月5日法務部第10603532 30號明確指出，原告既已收受警政署通報疑似有個資外洩一事，是否僅有網路釣魚詐騙案件，或仍有其他平台用戶資料外洩，於此階段尚無法得知仍須查明，依照前開函釋意旨，顯見其認為外洩事件尚在調查中而未臻明確，仍應就發現外洩情事通知當事人，甚者，原告既立於個人資料

控制管理者之地位，不得逕以其認知僅為網路釣魚詐騙案件，便免除個資法第12條個資事故通知義務，自應依法盡速通知受影響之資料當事人，並採取因應措施，使受損害之人數及範圍得受控制，避免其擴大，方為適法，以達到個資法保障當事人權益之意旨。原告稱個資法第12條規定不適用於網路釣魚詐騙案件，容有誤會。

3.又查，被告機關兩度函請原告就系爭通報案件做出妥善處理，並回報改善狀況，惟原告於111年11月8日、12月2日回函表示系爭通報案件為網路釣魚詐騙案件，復聲稱受害之當事人為平台用戶賣家，遂主張其不負個資法第12條個資事故通知義務，惟並未提出相關佐證資料，足以證明其無個資受侵害情事。然原告雖稱其於112年5月22日回函提供第三方獨立機構所出具之最新滲透報告，然其提出時點，顯為被告機關作成原處分1後，甚者，此最新滲透報告作成時點（即112年2月7日），亦為被告機關作成原處分1後，難以證明其於系爭通報案件期間(即111年9月至12月間），確無個資遭竊取、洩露、竄改或受其他侵害情事，故原告主張其於訴願決定1作成之前，已提出相關資料證明其平台無個資受侵害情事，實屬無稽。

㈡被告機關因認定原告未妥善執行適當安全措施，故為原處分2命原告限期改正之，固為適法，原告為相反主張云云，乃無理由：

1.被告曾函請原告說明「貴公司採行之個資安全措施」。原告於111年11月8日及12月2日回函僅聲稱系爭通報案件均屬網路釣魚詐騙案件，而未有個資外洩情事，並稱其採取如：於拍賣平台網站上公告提醒消費者注意詐騙事件、嘗試連結外部網站時會跳出相關警示畫面、偵測到異常登入情形時要求使用者輸入驗證碼進行雙重認證等安全措施，惟原告平台仍持續發生個資外洩事件，長居165專線公布之高風險賣場（平台），可見其回函所聲稱之適當安全措施未能有效保護個人資料安全，並未有效遏制系爭通報案

件持續發生及用戶之個人資料安全。再者，就我國個資法施行細則第12條第2項之個人資料盤點清冊、風險評鑑表、事故通報、教育訓練、稽核報告等佐證資料，原告均未能提出，尚難認已依個資法第27條第1項採行適當安全措施之義務。

2.被告機關因上述情事，遂於112年2月4日作成原處分2，命原告應限期改正依個資法第27條第1項，針對原告平台內使用者之對話視窗功能，採行有效阻斷QR Code及惡意連結之機制功能，並函請原告於原處分書達到之次日起2個月內完成改正，倘未於期限內回覆或經檢視改正不完全者，將依個資法第48條及第50條規定，視情節裁罰。原處分2敦促原告履行法律上義務，促請原告採取前述之適當安全措施，以適足保障資料當事人權利，內容洵屬明確，且有助於達成個人資料安全保護之目的，又網站平台屬於原告具有主控權之場域，該措施亦屬最小侵害手段，與為保護平台使用者個人資料之目的並無顯失均衡，亦符合比例原則。原告逕稱被告所命之該措施，詐騙集團仍可以各種變形符號突破，進而進行詐騙，該措施手段無助於目的之達成云云，顯係混淆原處分係為達成保護個人資料安全之目的，非防止詐騙事件之發生，原告認被告未加以區分防詐騙措施及安全措施，加以闡述該措施手段無助於目的之達成，是容有誤會等語，資為抗辯。並聲明求為判決：①駁回原告之訴。②訴訟費用由原告負擔。

五、本件如事實概要欄所載，有個資外洩電子商務業者清單（本院卷二第159頁至第241頁）、被告111年10月24日函（本院卷一第63頁至第65頁）、被告111年11月11日函（原處分卷第33頁至第35頁）、原告111年11月8日函、111年12月2日函（本院卷二第73頁至第108頁）、行政檢查會議紀錄、簽到表及行政檢查評核表（答辯二狀卷第27頁至第37頁）、原處分1（本院卷一第101頁至第102頁）、原處分2（本院卷一第105頁至第106頁）、訴願決定（本院卷一第15頁至第27頁）

等附卷可稽，兩造就此部分事實且無爭執，應可採為裁判基礎。故本件應審究之爭點為被告因原告個資外洩，認定原告違反個資法第12條及第27條第1項規定，命原告限期改正之處分是否適法？

六、本院之判斷：

㈠原告有即受確認判決之法律上利益：

1.行政訴訟法第6條第1項規定：「確認行政處分無效及確認公法上法律關係成立或不成立之訴訟，非原告有即受確認判決之法律上利益者，不得提起之。其確認已執行而無回復原狀可能之行政處分或已消滅之行政處分為違法之訴訟，亦同。」其立法理由載明：「……為防止濫訴，爰規定限於原告之權利或法律上利益有受侵害之危險，且得以確認判決除去者，始得提起之。」依上揭規定，提起確認訴訟，限於原告的權利或法律上利益有受侵害之危險，且得以確認判決除去者，始得提起之。而所謂即受確認判決之法律上利益，須因法律關係存否不明確，導致原告在公法上地位有受侵害之危險，且此項危險得以確認判決除去者，即屬存在。

2.本件依原告之主張，原處分因認定事實錯誤，而違法課予原告作為義務，縱使原告已依此改正完畢，被告仍可據以為後續之裁罰，被害人亦可能執此，以原告違反個資法為由，對原告提起民事侵權行為訴訟。故自原告主張之內容觀之，其確有可能因原處分違法與否，因兩造各執一詞，使法律關係陷於不明狀態，其權利或法律上利益有受侵害之危險，且得以確認判決除去之，是原告提起本件確認訴訴訟，應認具有確認利益及權利保護之必要。被告爭執原告提起本件確認訴訟並無確認利益，亦無權利保護必要等語，尚難憑採。

㈡本件相關法令：

1.為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定個資法。該法第

12條規定：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」第27條第1項規定：「非公務機關保有個人資料檔案者，應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。」行為時第48條第2款、第4款規定：「非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣2萬元以上20萬元以下罰鍰：……二、違反第10條、第11條、第12條或第13條規定。……四、違反第27條第1項或未依第2項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。」

2.法務部依個資法第55條規定授權訂定之個資法施行細則，其中第12條規定：「（第1項）本法……第27條第1項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。（第2項）前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：一、配置管理之人員及相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用之內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、使用紀錄、軌跡資料及證據保存。十一、個人資料安全維護之整體持續改善。」上開規定明定個資法第27條第1項應採取之技術上及組織上措施，核與母法及其他相關法規無違，可資適用。準此，非公務機關保有個人之個資檔案者，應採取與所欲達成之個人資料保護目的間，具有適當比例為原則，得包含上述事項之技術上及組織上的措施，以防止所保有之個資檔案被竊取、竄改、毀損、滅失或洩漏。

㈢被告認定原告有個資被竊取或洩漏情形，應屬有據：

1.本件係因警政署分別於111年9月13日、10月26日、11月30日，檢附個資外洩電子商務業者清單，函請被告就原告疑有違反個資法情事處理，此有警政署111年9月13日警署刑研字第00000000000號函、111年10月26日警署刑研字第00000000000號函、111年11月30日警署刑研字第00000000000號函暨所附之個資外洩電子商務業者清單卷內可稽（本院卷二第159頁至第166頁，第167頁至第201頁，第203頁至第241頁）。依據前述清單所載，經排除所載詐騙內容難以判斷類型之案件後，可大略區分為賣家受騙與買家受騙兩大類型，再據兩造自行統計，原告認為111年9月13日通報之65個案件中，賣家受騙有55件，買家受騙有6件；111年10月26日通報之321個案件中，賣家受騙為300件，買家受騙則有10件；111年11月30日通報之537個案件中，賣家受騙共512件，買家受騙為12件（參原證17，本院卷二第243頁至第246頁）。被告之統計結果則認111年9月13日通報之賣家受騙有56件，買家受騙有5件；111年10月26日通報之賣家受騙有295件，買家受騙有14件；111年11月30日通報之賣家受騙則有484件，買家受騙有16件（參被告答辯㈢狀，本院卷二第277頁）。兩造就警政署所通報案件之歸類雖略有出入，惟通報案件中均有買家與賣家受害，則無不同。

2.原告爭執警政署所通報之案件中，絕大多數均係以網路釣魚手法詐騙賣家主動提供個資，少數買家遭詐騙個案則未據被告舉證說明確因原告有個資被竊取或洩漏所致等情。本院查：

⑴關於買家受騙的情形：

①兩造一致認定屬買家受騙之案件（通報詐騙內容參附表）中，除極少數個案（111年10月26日通報案件編號182）外，受害情節均為買家曾在旋轉拍賣平台購物，嗣接獲詐騙電話以「訂單錯誤」、「分期付款」、「交易認證」、「帳號權限錯誤」、「重複扣

款」等話術取信後，買家依指示處置致轉帳而受損害。在此等案件類型，詐騙者通常係藉由提供與交易相關的真實資訊（例如交易標的、交易時間、交易價格、付款方式等）取信受害人，這也表示詐騙者已經由某種方式取得除買賣雙方外，僅交易平台即原告始能持有之前述交易細節。

②原告雖主張已採取包括採用Cloudflare Web Application Firewall過濾及監控HTTP流量保護網路應用程式、透過內部監控工具監控流量、設置Static Analysis Scanner掃描Pull Requests及防止個人資料外洩、由原告安全團隊人工檢視所有應用程式等資安防護措施，亦委請第三方獨立機構出具最新滲透測試等情，爭執被告並未舉證說明原告確有個資被竊取或洩漏。然買賣雙方在網路平台上進行交易所產生之數據資料，通常均存於平台業者支配領域中，若其不主動提供，行政機關獨立蒐集調查證據，不僅事所難能，縱可透過其他管道調查，亦將耗費鉅大行政資源與成本，故網路平台業者應擔負調查事實之協力義務。又旋轉拍賣平台之買家交易資訊確有遭他人取得並用以行詐之事實，業如前述；而上揭「訂單錯誤」、「分期付款」、「重複扣款」等詐騙話術，因長期以來迭有案例發生，政府機關乃至大眾傳播媒體亦常有宣傳報導，民眾較能警覺而避免受騙，則警政署歷次通報中，買家受騙類型雖僅佔全部通報案例之微小比例，考量「詐騙未遂」的黑數，本院認不應以買家受騙的通報案例數較少，即認買家受騙類型僅為零星發生的個案。被告主張原告有關於交易之個人資料被竊取或洩漏情形，亦堪支持。

⑵關於賣家受騙的情形：

①伴隨電信、網路科技發展，以電信通訊或網路作為實施工具之犯罪行為，尤其是詐欺犯罪大量發生，各國

莫不戮力偵辦防止電信詐騙、網路詐騙，從源頭攔阻詐騙訊息藉由電信通訊傳遞，即為其中要者。而攔阻詐騙訊息循電信通訊或網路傳遞，即需藉由公私協力方式，使民間業者承擔如核對確認發送訊息者身分、阻截詐騙或惡意訊息來源繼續發送等任務。又為防止個人資料被竊取、竄改、毀損、滅失或洩漏，非公務機關應採行適當之安全措施，個資法第27條第1項定有明文。所謂「適當之安全措施」雖屬不確定法律概念，惟依據非公務機關規模、特性、取得保有個人資料之性質及數量等因素，評估個人資料蒐集、處理、利用的流程，藉以分析可能產生的風險，並根據風險分析結果，訂定適當管控措施，實施後且應滾動檢討，就（疑似）發生個資被竊取或洩漏情形，採取應變措施以控制損害，查明事故狀況並以適當方式通知當事人，且應研議預防機制防止類似事故再次發生等，均應屬之。

②警政署所通報案例，其絕大多數均屬賣家受騙類型，具體情況略為：詐騙者佯裝買家，向賣家宣稱因賣場未完成驗證而無法成功下單，並出示結帳失敗的系統通知，要求賣家以Line等App掃描前述系統通知訊息所附QR Code聯絡客服人員辦理更新；或詐騙者直接以Line App與賣家聯絡，告以上述無法成功下單等情，要求賣家與客服人員聯繫處理。待賣家掃描QR Code連結至假冒之線上客服、外部網站或平台，或藉由Line App與假冒之客服人員聯繫後，詐騙者再誘騙賣家提供個人資料與/或銀行帳戶資訊。此據原告111年11月8日、12月2日發函向被告說明，並有原告提供之詐騙訊息截圖可稽（本院卷二第73頁至第108頁），被告就此部分事實且無爭執，則原告主張賣家受騙類型係屬「網路釣魚」之詐騙模式，為賣家主動提供個資予詐騙者等情，並非無據。

③惟原告做為網路拍賣平台，為網路交易服務的提供者，不問係為建構安全交易空間以保護買賣雙方，或追求交易平台之永續經營，對於「網路釣魚詐騙」均有採取適當且有效之預防、通報及應變機制的作為義務。查被告自接獲警政署通報起，先後於111年10月24日、11月11日發函要求原告查明妥處並提供相關佐證資料，原告回函雖說明個資可能外洩原因、對當事人之通知、事故後續處理作為及採行之個資安全措施等，惟觀諸警政署通報結果，第1次通報（統計期間為111年7月30日至8月28日）被害件數為65件，第2次通報（統計期間為111年9月17日至10月16日）被害件數為324件，第3次通報（統計期間為111年10月25日至11月24日）被害件數則達538件，呈現遞增趨勢，顯示原告所採行措施尚未發生阻止或減少詐騙案件發生的效果。迄被告於111年12月30日召開行政檢查會議，經原告出席說明後，被告評核結果認定原告涉有違反個資法第48條規定，應限期改正2個月，另建議原告「買賣家聊天功能應阻斷導向外部連結及封鎖QR Code圖片，應主動針對聊天內容之特定文字封鎖，如『簽署』、『協定』、『金流』、『添加客服』、『系統通知』、『凍結』……」（答辯二狀卷第27頁、第37頁），原告則於原處分作成後以112年3月21日函通知被告稱已透過電子郵件通知用戶、且已採行阻斷QR Code及惡意連結之機制等功能（本院卷一第109頁至第114頁），而被告於本院審理時亦稱「……經被告的要求及原告進行、提供相關保障措施後，原告經營的拍賣平台上受詐騙的情形已有減少……經過原告之改善，就詐騙事件也產生了防堵的效果，數量已經大幅下降……」等語（本院卷二第319頁），可認被告所建議之「阻斷外部連結、封鎖QR Code」確為有效方法。衡諸上情，並考量遭詐騙之賣家，顯然

認為詐騙者佯裝買家出示前述結帳失敗、系統通知等訊息確為原告之「官方通知」，亦不瞭解該訊息所含QR Code或Line App係導向外部連結，原告作為交易平台業者，仍應採取必要的「防笨措施」以防止使用者發生個資被竊取或洩漏情事。本院因此沿襲既有判決前例（本院112年度訴字第1396號）立場，支持被告所認上述賣家受騙類型亦該當原告所保有個人資料被竊取或洩漏之見解。

㈣被告依個資法第48條第2款、第4款規定命原告限期改正，於法並無違誤：

1.被告自警政署111年9月13日通報後，即於111年10月24日發函原告以「為調查本案，請貴公司於文到15日內就下列事項函復說明，並檢附相關佐證資料：……㈡對當事人（即會員、消費者等）之通知，就本次事故是否查明後以適當方式通知當事人，內容至少應包括個人資料被侵害之事實及已採取之因應措施，請檢附通知內容（非防詐騙宣導等預防性通知，個資法第12條及其施行細則第22條參照……）」、「……如有違反個人資料保護法第27條第1項及同法施行細則第12條第2項規定之情事，倘查證屬實，依同法第48條規定，應限期改正……」、「本部依據個資法第27條第3項規定定有『網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法』（按已於112年11月21日廢止），亦請卓參，並請依該辦法規定辦理。」，應認已有原告應遵循個資法第12條及第27條第1項行政法上義務之明文通知。

2.惟依原告111年11月8日、12月2日回函，均稱「本公司調查後，沒有跡象顯示本公司系統被駭客入侵或有個人資料被竊取、洩漏、竄改或其他侵害之情形，因此並無個人資料保護法第12條規定應通知當事人之情

形。……本公司為了保護旋轉拍賣網站的使用者，乃自111年1月起陸續採行下列措施：⑴針對使用者舉報的詐騙行為，在旋轉拍賣網站刊登明顯公告，提醒使用者『切勿相信不明假客服連結、QR Code或LINE帳號』……⑵使用者透過本公司網站或應用程式進行對話時，如果對話內容出現特定關鍵字或QR Code二維碼時，本公司網頁將自動跳出安全警示。如果使用者嘗試連結到本公司網站或應用程式以外的外部網站，也會出現外部連結警示畫面，請使用者確認是否確實要連結至外部網站。……⑶本公司已於網站首頁設置橫幅標語警示使用者，使用者進入網站便會看到該則橫幅標語。此外，系統偵測到使用者帳號有異常登入情形時，便會寄發電子郵件要求使用者輸入驗證碼進行雙重驗證……」等語，可知原告確實未依被告上開函文說明，以「非防詐騙宣導等預防性通知」之適當方式通知當事人其個資被侵害之事實及已採取之因應措施等。至於其他防止個資被竊取或洩漏之安全措施，在確實阻斷外部連結及封鎖QR Code前，復未生實際效果，亦如前述，則被告以原告違反個資法第12條、第27條第1項規定，分別以原處分1、原處分2命原告限期改正，於法尚無違誤。

七、綜上所述，本件原處分並無違誤，訴願決定遞予維持，亦無不合，原告所爭執各節，均不採取，其訴請確認原處分為違法，為無理由，應予駁回。

八、本件事證已臻明確，兩造其餘攻擊防禦方法及訴訟資料，經核均與本件判決結果不生影響，故不逐一論述，併此敘明。

據上論結，本件原告之訴為無理由，依行政訴訟法第98條第1項前段，判決如主文。

中　　華　　民　　國　　114　　年　　1　　月　　9　　日

審判長法　官　蕭忠仁

法　官　許麗華

法　官　吳坤芳

一、上為正本係照原本作成。

二、如不服本判決，應於送達後20日內，向本院高等行政訴訟庭提出上訴狀，其未表明上訴理由者，應於提出上訴後20日內補提理由書；如於本判決宣示或公告後送達前提起上訴者，應於判決送達後20日內補提上訴理由書（均須按他造人數附繕本）。

三、上訴未表明上訴理由且未於前述20日內補提上訴理由書者，逕以裁定駁回。

四、上訴時應委任律師為訴訟代理人，並提出委任書（行政訴訟法第49條之1第1項第3款）。但符合下列情形者，得例外不委任律師為訴訟代理人（同條第3項、第4項）。

得不委任律師為訴訟代理人之情形	所需要件
(一)符合右列情形之一者，得不委任律師為訴訟代理人	1.上訴人或其代表人、管理人、法定代理人具備法官、檢察官、律師資格或為教育部審定合格之大學或獨立學院公法學教授、副教授者。 2.稅務行政事件，上訴人或其代表人、管理人、法定代理人具備會計師資格者。 3.專利行政事件，上訴人或其代表人、管理人、法定代理人具備專利師資格或依法得為專利代理人者。
(二)非律師具有右列情形之一，經最高行政法院認為適當者，亦得為上訴審訴訟代理人	1.上訴人之配偶、三親等內之血親、二親等內之姻親具備律師資格者。 2.稅務行政事件，具備會計師資格者。 3.專利行政事件，具備專利師資格或依法得為專利代理人者。 4.上訴人為公法人、中央或地方機關、公法上之非法人團體時，其所屬專任人員辦理法

	制、法務、訴願業務或與訴訟事件相關業務者。
是否符合(一)、(二)之情形，而得為強制律師代理之例外，上訴人應於提起上訴或委任時釋明之，並提出(二)所示關係之釋明文書影本及委任書。	

中　　華　　民　　國　　114　　年　　1　　月　　9　　日

書記官　何閣梅