附件四

時報文化出版企業股份有限公司

個人資料保護管理辦法

104.4.22 修訂

壹、目的

為確保本公司在使用個人資料時符合「個人資料保護法」，從個人資料的蒐集、處理及利用能有效進行管理與保護，特制訂本辦法。

貳、範圍

本辦法適用於全公司所有人員。

參、權責

一、個資保護管理小組

1. 不定期向全體同仁宣導個人資料保護之相關程序與緊急應變之因應措施，並督導個資保護相關管控程序與落實執行。
2. 個資保護與管理業務等之協調連繫、個資安全事件通報以及重大個資外洩事件對外連繫等作業。
3. 依相關法令協調整合本公司個資保護及管理事項，並提供連絡方式及管道于個資當事人對個資請求事項及回應。

二、全公司所有同仁

1. 蒐集、處理及利用時應確認所使用之個人資料符合以下情形:
   i. 僅限執行所屬職務必要範圍內，對於非職務所需之個人資料應避免蒐集與使用。
   ii. 使用前須先取得當事人書面同意、契約同意或電子簽章同意。
   iii. 對當事人權益及隱私無侵害。

肆、作業程序

一、建立當事人通知管道

1. 建立對個資當事人的通知管道，如書面通知、電子郵件通知、電話通知、口頭通知、隱私權聲明或個資作業公告，並依本公司「個資蒐集、處理及利用告知暨同意書」告知當事人個資行使之權利及方式。網站讀者則於本公司網站中「時報悅讀網服務條款」進行告知。

二、個人資料蒐集

1. 直接蒐集資料應先告知當事人使用目的、範圍及對其權益之影響，並取得書面同意、契約同意或電子簽章同意，並每一年定期進行個資盤點。
2. 向第三方蒐集資料應建立契約或協議，使用外部其他單位資料庫或網站資料等其他來源的個資，應簽署資料交換契約或協議。

三、個人資料處理

1. 個人資料處理包含記錄、輸入、編輯、更正、輸出、儲存、複製、傳輸、刪除與報廢等作業。
   i. 記錄、輸入、編輯、更正與輸出
      甲、記錄、輸入、編輯及更正個資，應先提出申請「應用系統帳號及權限申請單」勾選個人資料類別及處理方式，進行資料審核並留下紀錄。
      乙、業務處理過程中產生與使用個資之資料及報表，應依資料類別標示第 4 級最高機密等級，並僅供已授權單位或人員使用。
      丙、資料輸出報表與交換使用，應先提出申請「應用系統帳號及權限申請單」勾選個人資料類別及處理方式，經主管及個資保護管理小組核可並保存相關紀錄。
      丁、因可歸責於本公司的事由而未進行更正或補充之個資，應於更正或補充後，通知當事人。
   ii. 儲存與複製
      甲、含個資之書面文件與多媒體儲存設備存放時，除已經以任何方式公開之個資外，需加鎖或以管制區域保護，避免遭人任意檢視或拿取，僅開放給授權存取之人存取，並不可在公開場合使用。
      乙、個人使用含個資之書面文件與多媒體儲存設備時，確實遵守安全保護要求，離座或下班時不可遺留於桌面或機器設備上。
      丙、含個資之書面文件與多媒體儲存設備，未經單位主管同意並作成紀錄不得攜帶外出或拷貝複製，應先提出申請「應用系統帳號及權限申請單」勾選個人資料類別及處理方式並留下記錄。

丁、多媒體儲存設備在媒介上依資料類別標示第 4 級最高機密等級，磁碟片貼上紅色圓貼紙，CD 光碟片，則以手寫方式直接書寫於 CD 光碟片上。

戊、電子檔案存放時以硬體設備或加密方式保護，檔案伺服器放置個人資料時設定權限控管，避免遭人任意檢視或拿取。

己、個人使用個資電子檔案時，確實遵守要求，離座時需啟動電腦螢幕保護裝置，下班時除非特殊考量，需將個人使用設備關機或加鎖保護。

庚、重要個資備份應放置倉庫異地存放，並置有防火設備，以防止資料滅失或遭竊取。

iii. 傳輸

甲、書面文件與多媒體儲存設備於內部人工傳送時，請親自傳送或經由授權核准的職務代理人傳送。

乙、書面文件與多媒體儲存設備以紙本郵件方式傳送到外部時，須以雙信封封存，並於內封加蓋「密」字，再以掛號方式寄出。

丙、書面文件掃瞄、列印、影印或傳真時，不可任由文件遺留於機器上，如經查獲違反規定者交由個資保護管理小組懲處。

丁、個資電子檔案應盡量避免以 e-mail 或 FTP 等電子傳送方式，若特殊需求，須加密始得傳輸，使用壓縮技術及設定密碼。密碼可透過電話告知或另外發一封 e-mail 告知，勿打在同一封 e-mail 內。

iv. 刪除與報廢

甲、書面文件之資料，除已經以任何方式公開之個資外，一律使用碎紙機將文件銷毀。

乙、多媒體儲存設備須報廢或不堪再使用時，依媒介性質則由個人或資訊單位人員以燒毀、粉碎或使用其他應用程式或工具清除資料或銷毀該媒介。

四、個人資料利用

1. 應明確界定本公司執行相關業務服務或為行銷或研究調查目的之使用的必要範圍，包括業務承辦單位與受委託單位。
2. 利用個人資料對當事人進行第一次行銷或研究時，應提供當事人拒絕行銷或研究的機制，可以電話或 e-mail 方式拒絕。

五、國際傳輸

如因業務需求需將個人資訊移轉到本國以外的地方，需確保個資的處理與利用符合本國法令規範並受到本辦法之相關作業保護。

六、個人資料蒐集特定目的消失或期限屆滿之處理方式

1. 應定期檢視個資是否為執行職務或業務所必須資料，或已經當事人書面同意者，並登錄於個資類別清單(讀者、作者、員工、股東及其他)。
2. 應定期檢視個資項目是否可能發生特定目的消失或期限屆滿事件，如可能發生則應確認是否為執行職務或業務所必須資料，或已經當事人書面同意者，而可以停止代替刪除。否則應準備個資刪除、停止處理或利用個資相關作業。
3. 經檢視若非職務或業務所必須資料，但仍有保留處理與利用之需求，則應於期限屆滿前取得當事人書面同意。
4. 個資蒐集之特定目的消失或期限屆滿，而需進行刪除作業者，依照個資處理-刪除與報廢程序進行，應確認該項資料已完成刪除作業，並留下相關的紀錄與證據。

七、個人請求資訊

1. 請求項目

i. 提供當事人資料，其流程應包含下列事項：

甲、查詢或閱覽

乙、製給複製本

丙、補充或更正

丁、停止蒐集、處理或利用

戊、刪除

ii. 若當事人要求答覆查詢、提供閱覽或製給複製本等事項，涉及下列情況，則可依規定不提供該項請求：

甲、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。

乙、妨害公務機關執行法定職務。

丙、妨害該蒐集機關或第三人之重大利益。

2. 請求與駁回期限

i. 受理當事人個資之答覆查詢、提供閱覽或複製本等請求項目，應於十五日內，完成同意處理或駁回的決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。

ii. 受理當事人個資更正或補充請求，應於三十日內，完成同意處理或駁回的決定；必要時， 得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。

3. 請求流程

i. 當事人填寫「個資請求申請表」，如為代理人申請則須附委託同意書。

ii. 親送或寄至本公司個資保護聯絡窗口。

iii. 個資保護聯絡窗口先進行身份查驗、核對及確認，並依據業務類別轉至個資保護管理專責人員進行相關處理。

iv. 查詢或請求閱覽個人資料或製給複製本者，如須繳交費用，則依本公司繳費方式進行繳費。

4. 請求管理作業

i. 資料查詢或閱覽

甲、由業務承辦人員先進行身份查驗、核對及確認當事人後提供查詢結果，或請當事人至本公司進行資料閱覽，亦可在安全控制下提供線上查詢或閱覽。

乙、提供複製本

■ 由業務承辦人員於申請單陳核後依據申請人選擇方式交付文件，取件方式如下：

✧ 親自領取並核對證件如下：

➢ 本人申請：身分證正本。

➢ 由代理人(配偶、父母、成年子女)申請：當事人身分證正本、代理人身分證正本及當事人之委託書。

➢ 未成年人由法定代理人申請:法定代理人身分證正本、法定代理人與當事人關係證明文件(戶口名簿或當事人身分證正本)。

- 郵寄方式：郵寄至申請人指定之地點，須繳納掛號郵資 。

■ 補充或更正

✧ 由業務承辦人員先進行身份查驗、核對及確認當事人後，應查明其資料是否正確，如為正確資料 ，應於經呈核後進行補充或更正作業。

■ 停止蒐集、處理或利用

✧ 由業務承辦人員先進行身份查驗、核對及確認當事人後，查明是否為依法規或執行職務或業務所必須之資料，若為必須之資料而無法停止，則應以書面函覆當事人說明原由，以取得瞭解。非必須之資料，則於呈核後進行停用作業。

■ 刪除

✧ 由業務承辦人員先進行身份查驗、核對及確認當事人後，查明是否為依法規或執行職務或業務所必須之資料，若為必須之資料而無法刪除，則應以書面函覆當事人說明原由，以取得瞭解。非必須之資料，則於陳核後進行刪除作業。

5. 請求駁回作業

i. 所有請求如依據規定或因執行職務或業務所必需，而無法同意其請求，均應以正式書面函覆，並以掛號方式寄出。

ii. 函覆內容應包含申請項目、駁回原因、申訴管道及相關連絡資訊。

八、設備管理-資訊應用系統安全

1. 處理含個資之資訊應用系統應符合「資訊安全管理辦法」，檢視並建立具有保護個資機密性、完整性、可用性與不可否認性等安全機制。其作業包含:

i. 系統開發與建置

甲、規劃資訊系統的個資保護的安全要求，如權限控管功能、系統稽核功能及完善系統文件。

乙、建立記錄、輸入、編輯、更正及刪除等資料驗證及錯誤更正的機制。

丙、系統輸出之資料及報表，依權限與報表使用之性質設定使

用者權限，並區分使用者合理所需的個資內容及資料欄位，並僅供已授權單位或人員使用。

丁、資料輸出與交換使用應經核可並保持相關記錄。

戊、建立資料輸入、運算與輸出控制應相互配合機制，並與程式控制中需有適當之檢查方式。

己、系統建置階段即應同時於系統中建立安全機制，如權限控管功能、系統稽核功能及完善系統文件。

ii. 系統使用

甲、使用資訊應用系統應建立記錄、輸入、編輯及更正等資料審核流程及資料錯誤更正的作業程序，並明定資料輸入與異動過程中相關人員的責任。

乙、系統內記錄、輸入、編輯及更正等作業應定期進行審查，以確保資料的正確性與完整性。

丙、系統產生的資料或報表應確認標示機密等級，並僅供已授權單位或人員使用，資料輸出、報表與交換使用應經核可並保存相關記錄。

iii. 系統資料交換與連結

甲、資訊系統如連結外部其他單位的資訊系統或資料庫時，應注意僅能使用於已告知且相容的目的資料，並先取得雙方資料交換協議。

iv. 系統稽核

甲、經要求系統產生系統稽核日誌，記錄內容應包括使用者帳號、登入登出之日期時間、動作指令、執行結果、電腦的識別資料或其網址及事件描述等事項。

乙、系統稽核記錄每月應作備份至少需保存 5 年，禁止未經授權之刪除及修改，以作為日後稽核調查及監督之用。

v. 系統備份與還原

甲、系統資料應定期執行備份作業，由負責人員檢視備份結果，追蹤備份失效之原因並改善直到確定所有備份作業成功。

乙、各系統主機之資料備份至少保留三代。

丙、每年進行一次資料還原測試並作記錄。

丁、應建立系統毀損之回復作業程序及應變措施。

九、設備管理-資訊設備安全

1. 設備使用與維護
   i. 建置個資之個人電腦，不應直接作為公眾查詢工具。
   ii. 資訊設備應注意資料備份及相關安全措施。
   iii. 移動或攜出含個資之資訊設備，應申請核准並留下紀錄。
   iv. 建置或處理個資之個人電腦，經 e-mail、USB 或其他多媒體儲存設備的個資使用需經「個資使用多媒體儲存設備申請表」核准並留下記錄。
2. 設備報廢
   i. 處理電腦設備報廢應符合「電腦設備報廢管理辦法」，設備超過年限或無法修理申請報廢、轉售或廢棄者時應經權責主管核准後，請資訊單位刪除資產所儲存之相關資料。並視情況需要使用適當工具再次進行資料清除作業。
   ii. 資訊系統儲存媒體損壞、無法執行其功能或無需繼續保存使用時，應銷毀該儲存媒體。

十、其他安全維護事項

1. 密碼管理
   i. 個資檔案應釐定使用範圍及使用權限，密碼應保密不得與他人共用。
   ii. 個人密碼應保密，且須每 90 天定期變更密碼，以防被竊取使用。
2. 個人電腦儲存個資檔案者時，應設定登入密碼、啟動螢幕保護程式及安裝防毒軟體等安全措施。

十一、 資料稽核

1. 個資管理單位應定期及不定期稽核個人資料檔案管理情形。
2. 以電腦處理個資時，應檢視記錄、輸入、編輯、更正及刪除是否與原檔案相符。
3. 個資提供使用時，應核對與檔案資料是否相符，如有疑義，應調原檔案查核。
4. 個資保護管理小組指派個資稽核人員定期檢核含有個資之資訊設備使用者之權限清單，確認使用者對資訊存取是否符合規範，實施稽核時，得調閱有關資料，並請相關處理人員說明。個資稽核人員每年須經稽核專業訓練。

十二、 記錄與證據之保存

1. 所有的事件紀錄，包含紙本或電子形式，應放置於安全處所或安全的儲存設備，並依業務權限控管，以防止非授權人員的塗改或破壞。
2. 事件紀錄表單應加以審查，並經相關主管核備後保存。
3. 審查事件紀錄表單時須特別注意其完整性及是否有任何異常，並追蹤其原因，留下稽核紀錄。電腦稽核軌跡及相關的證據，每月應作備份至少需保存 5 年，禁止未經授權之刪除及修改，以為日後稽核調查及監督之用。

十三、 人員管理及教育訓練

1. 員工安全管理
   i. 員工報到時，應要求其閱讀「時報員工工作規則」、「個人資料保護管理辦法」及「資訊安全管理辦法」並充分瞭解個資保護與資訊安全相關規定，並簽署「個資蒐集、處理及利用告知暨同意書」。
   ii. 員工執行業務時，遵守政府個人資料保護法及資訊安全相關法令及本公司個資保護與資訊安全相關規定，若違反時應依相關法令及本公司相關規定懲處。
   iii. 員工離職時，依據「員工離職經辦事項表」及「移交清冊目錄」辦理各項離職相關事宜，包括帳號及權限停用或刪除。
   iv. 處理個資檔案人員職務異動時，應將所保管之儲存媒體及有關資料列冊移交，接辦人員應另行設定密碼以維護安全。
   v. 員工離職後，其離職員工曾接觸過之密碼均需取消或更改為新密碼。
2. 個資保護教育訓練
   i. 應定期及不定期對各單位實施個資安全防護教育訓練。
   ii. 包含個資保護觀念及作法宣導、法律相關規範及正確使用資訊設備等。

十四、 受委託單位管理

1. 受委託單位契約要求
   i. 針對受託單位的各項管理措施均應明文規範於委外合約或相關契約文件中。
2. 有關個資處理之相關作業，均依本辦法之規定辦理，且接受本公司

相關稽核作業。

十五、 緊急應變措及通報

1. 安全事件通報

i. 發現個資被竊取、洩漏、竄改、毀損、滅失或其他侵害事件，應先通報個資保護管理專責人員。

ii. 判定事件狀況後，由個資保護管理專責人員依事件輕重等級呈報經營管理階層。

2. 安全事件處理

i. 事件發生後，應立即進行矯正預防措施，事件處理時間應於指定時間完成，作業內容應記錄備查，並經由相關權責人員審視確認。

ii. 事件處理前，應先備份數位證據如系統記錄及稽核軌跡等，確實做好證據保存工作。

iii. 應鑑別事件發生根本原因，以利事件處理作業，如為外來攻擊事件，應適當鑑別攻擊來源。

iv. 如發現可能為資訊系統漏洞或脆弱點，應通知資訊室協助以獲得解決方案，並執行修復作業。

v. 完成事件處理後，應提供處理結果報告，交由個資保護管理小組彙整報告個資當事人及公司經營管理階層。

十六、 個人資料檔案盤點

1. 個資保護管理小組每年應至少辦理一次個人資料檔案盤點作業，以確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理或利用之個人資料之類別或範圍。

2. 凡業務或日常作業涉及個人資料蒐集、處理與利用之部門應參與個人資料檔案盤點作業，並建立個人資料檔案盤點清冊。

3. 於個人資料檔案盤點時，發現有非屬特定目的必要範圍內之個人資料或特定目的消失、保存期限屆滿而無保存必要者，應依本辦法所定程序，刪除、銷毀或停止處理或利用該個人資料。

4. 於法令修定或有必要時，個資保護管理小組得適情況決定是否辦理個人資料檔案盤點作業，相關部門應參與個人資料檔案盤點作業，並建立或調整個人資料檔案盤點清冊。

5. 個人資料檔案盤點清冊應於參與個人資料檔案盤點作業相關部門主管簽名確認及總經理核定後，送管理部保存；於有調整時，亦同。

十七、 資訊安全稽核機制

1. 內部稽核人員訂定年度稽核計畫應包含資訊系統循環及資通安全檢查，並依計畫執行稽核工作與撰寫稽核報告並呈董事長核准；若發現內控缺失及異常事項，應加以追蹤並做成追蹤改善報告，經適當之權責主管複核，並適時予以解決，並於董事會提出報告，以確保內部控制制度執行之有效性。
2. 稽核人員每年定期執行個人資料管理專案計畫之稽核，查核依一般性內部稽核工作方式，報告採專案處理方式，會簽個人資料保護與管理執行小組之組織成員並呈總召集人核准後，通知各受查之單位改善，並做成追蹤報告經總召集人複核，以確定其已即時採取適當之改善措施。

十八、 改善建議

1. 執行時機 – 當內部及外部稽核發現缺失或是發生個資安全事件時，應進行原因分析與改善措施。
2. 進行原因分析 – 應分析問題發生之原因及影響程度，決定優先順序與處理時限。
3. 提出改善對策 –提出改善措施時，得區分為暫時性對策或永久性對策，防止類似事件發生，並應考慮成本效益及可行性。
   追蹤執行狀況 –各項改善措施計劃應指派人員追蹤，並應於改善措施計劃上留存追蹤記錄。個資保護管理專責人員彙整相關改善措施之執行狀況，於個資保護管理小組會議提出報告。