

# 臺北市政府資訊局個人資料保護管理要點

101年8月14日北市資綜字第10130334000號函訂定，並自101年9月18日起生效  
101年10月3日北市資綜字第10130397700號簽奉核定修正

## 壹、通則

- 一、臺北市政府資訊局（以下簡稱本局）為落實個人資料蒐集、處理或利用符合法令、尊重當事人資訊自決權、促進個人資料合理利用及避免人格權受侵害，特依個人資料保護法（以下簡稱本法）及國際組織所揭示原則或規範，訂定本局個人資料保護管理要點（以下簡稱本要點）。
- 二、本要點名詞，定義如下：
  - （一）書面同意：指紙本同意文件或依電子簽章法經當事人同意電子文件。
  - （二）高風險個人資料：指本法第六條以外對當事人之人身或財產安全、隱私或資訊自決權影響較大之個人資料。
    1. 個人財務資料或交易紀錄，如信用卡資料、網上交易細節。
    2. 政府核發辨識資料，如身分證號碼、護照號碼。
    3. 個人生物特徵識別資料，如指紋、臉部特徵資料。
    4. 其他可能侵擾個人生活秘密空間之資料。
  - （三）去識別化：指個人資料經過處理（如代碼、匿名、隱藏部分資料、模糊化處理等）後達到無法識別特定個人程度。
  - （四）各組室：指本局各組、室。
  - （五）其他單位：指本局以外之法人（機關、廠商）、團體或自然人。
  - （六）專人：指依本法第十八條所指定負責個人資料保護業務專責人員。

三、本要點適用於本局及受本局委託或與本局共同蒐集、處理或利用個人資料之其他單位，但其他法令另有規定者，從其規定。

## 貳、保障當事人資訊自決權及公眾查閱權利

- 四、當事人依本法第十條或第十一條第一項至第四項規定向本局請求答覆查詢、提供閱覽、製給複製本、更正、補充、停止蒐集、處理、利用或刪除個人資料時，應經身分確認程序後，本局得視情形請當事人檢附相關證明文件或為適當之釋明。

前項文件內容如有遺漏、欠缺或釋明不完整，應通知限期補正。  
申請案件有下列情形之一者，應以書面或電子文件駁回其申請：

  - （一）申請書件內容有遺漏、欠缺、虛偽不實或釋明不完整，經通知限期補正，逾期仍未補正或無法補正。
  - （二）有本法第十條但書各款情形之一。
  - （三）有本法第十一條第二項但書或第三項但書所定情形之一。

(四) 與法令規定不符。

處理時程依本法第十三條規定辦理。

五、當事人請求閱覽、抄錄、攝影、製給個人資料複製本，適用臺北市政府及所屬機關學校提供政府資訊收費標準收取費用。

當事人閱覽其個人資料，應由承辦組室派員陪同為之，並適用或準用臺北市政府及所屬各機關大專院校檔案開放應用要點。

六、各組室提供當事人閱覽、抄錄、攝影、製給其個人資料前，應確認未同時揭露他人個人資料。

七、為確保當事人有充分表達意見機會及申訴管道，本局網站之個人資料保護專區設置個人資料客訴聯絡方式。

八、本局保有個人資料檔案以公開於機關網站之個人資料保護專區為原則，公開時間以建立個人資料檔案後一個月內為之；更新檔案時亦同。

### 參、蒐集

九、各組室蒐集或處理個人資料應符合下列情形之一：

(一) 依本局組織規程或本法第十五條第一款及本法施行細則第十條所稱執行法定職務。

(二) 經當事人書面同意。

(三) 依法受委託執行職務。

受委託執行職務前，應確認委託蒐集或處理個人資料之適法性及合理性。有疑義時應即通知委託人。

十、各組室蒐集個人資料時應註明蒐集用途，即特定目的項目及代號。

十一、各組室蒐集個人資料應符合本法第五條比例原則，以處理業務必要範圍內為之，儘量以蒐集最少且不含高風險個人資料類別為原則。

十二、經當事人書面同意者，應依本法第八條第一項告知當事人蒐集目的、資料類別、利用相關事項、當事人所得行使之權利等事項，但有本法第八條第二項情形者，不在此限。

告知事項內容應使用通俗、簡淺易懂之文字，避免使用艱深費解之詞彙，以確保當事人在知情下同意 (informed consent)。如有委託或共同蒐集、處理或利用個人資料，應同時告知委託或共同利用情形。

告知方式得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。

十三、各組室所蒐集之個人資料非由當事人提供者，應於處理或利用前，向當事人告知資料來源及本法第八條第一項所列事項，但有本法第九條第二項情形者，不在此限。

十四、對滿七歲之未成年人蒐集或處理其個人資料，有下列情形之一者，得經未成年人本人書面同意為之，其他情形應得其法定代理人書面同意。

- (一) 依其年齡及身分、日常生活所必需。
- (二) 純獲法律上利益（純粹取得權利或不負任何義務）。
- (三) 法定代理人事前允許處分財產或營業。

對未滿七歲之未成年人及受監護或輔助宣告之人蒐集其個人資料，應得其法定代理人書面同意。

法定代理人基於保護未成年人及受監護或輔助宣告之人之利益，得行使本法第十條或第十一條第一項至第四項規定之權利。未盡事宜依民法及兒童及少年福利與權益保障法等相關規定辦理。

#### **肆、處理或利用**

十五、各組室處理或利用個人資料應符合本法第五條比例原則，利用個人資料類別、數量及接觸人員以處理業務必要範圍內為限。

十六、各組室應優先考慮以去識別化或經遮蔽之個人資料為處理或利用。

十七、個人資料正確性有爭議時，應停止處理或利用並註明。

十八、個人資料有補充、更正、停止處理或利用、刪除時，應通知曾利用之其他單位；或與其他單位事先協調及規劃個人資料定期更新機制。

十九、任何非原蒐集目的之特定目的外利用，應依本法第十六條但書確認或審查後處理或利用，並視具體情形規劃當事人得選擇不同意機制。

二十、各組室將個人資料作國際傳輸前，應確認法令限制及他國（境）對個人資料保護法令要求，並為適當保護措施。

#### **伍、安全維護**

二十一、電子處理之個人資料安全維護，依行政院及所屬各機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範、行政院國家資通安全會報技術服務中心所訂各項資訊安全參考指引、本局資訊安全政策及相關規範辦理。

非電子處理之個人資料安全維護依臺北市政府文書處理實施要點、臺北市政府公務機密維護作業規定辦理。

本局得因應最新技術發展或資訊安全問題訂定技術指引。

各組室得因應負責業務特性自訂內部安全控制措施或管理細則。

二十二、個人資料風險評估必要項目如下：

- (一) 個人資料可識別程度。

- (二) 個人資料數量。
- (三) 個人資料類別敏感性及風險性。
- (四) 蒐集、處理、利用過程及環境。
- (五) 個人資料保護意識及義務程度。
- (六) 個人資料存取頻率及存放位置。

各組室得依個人資料所使用資通訊技術之風險特性或業務性質增訂評估項目，並得參考資訊安全業務內部控制制度共通性作業範例辦理。

二十三、使用任何工具、軟體或服務時，應確認未含自動記錄個人資料或侵害隱私功能。

二十四、各組室應視業務性質保存下列紀錄或證據：

- (一) 當事人書面同意。
- (二) 告知或通知當事人。
- (三) 當事人或法定代理人依本法第十條或第十一條第一項至第四項規定主張權利。
- (四) 蒐集、處理、利用個人資料所生之軌跡紀錄檔 (log files)。
- (五) 本局或各組室之檢查或稽核。
- (六) 本要點第三十三點之監督紀錄。
- (七) 個人資料正確性有爭議。
- (八) 個人資料被竊取、洩漏、竄改或其他侵害事故。

二十五、負責蒐集、處理或利用個人資料之職員工或其他單位員工，應定期參加資訊安全或個人資料保護教育訓練。

新進職員工或參與本局招標第一次得標廠商員工，應詳閱本局個人資料保護相關規範或參加教育訓練。

專人不定期通知個人資料保護注意事項，各組室視情形轉知業務相關其他單位。

二十六、各組室每年至少一次自行辦理個人資料風險評估。

本局每年依臺北市政府及所屬各機關辦理資訊使用管理稽核作業規定辦理內部及外部稽核。

本局每年應依網站資料檢核計畫辦理二次機關網站及主題網站檢核。

二十七、為妥善因應個人資料安全事故，各組室平時應建立通報及支援聯絡網人員名冊，掌握個人資料處理或利用流程，透過監測資料注意異常狀況之潛在問題。

二十八、個人資料被竊取、洩漏、竄改或其他侵害事故發生時，以知悉時起二小時內完成通報作業。通報對象包括局長、主任秘書、事故組(室)主管、政風人員、專人或以上人員之代理人。通報內容至少包括通報人身份、資料外洩或侵害方式、

時間、地點、初估外洩或侵害個人資料類別及數量、避免損害擴大處置等資訊。通報方式以電話或簡訊為主，電子郵件為輔。

二十九、事故組（室）於知悉時起四小時內，依指示及視事件性質進行包含下列內容之應變措施：

- （一）中斷入侵或洩漏途徑。
- （二）緊急儲存尚未被破壞資料。
- （三）啟動備援程序或替代方案。
- （四）事故原因初步分析。
- （五）評估受侵害個人資料類別及數量。
- （六）檢視防護及監測設施功能。
- （七）記錄事故經過。
- （八）行政內部調查完成前保存相關證據。
- （九）解決或修復方案。
- （十）通知保有相同資料組室或其他單位。
- （十一）洽商專業人員協助或進駐處理。
- （十二）涉及刑事責任者，移請檢警鑑識或調查。
- （十三）發布新聞稿、網站公告及通知當事人。

前項四小時辦理時間，必要時得經授權延長。

三十、事故查明後依本法第十二條通知當事人，內容包括侵害事實及因應措施說明、建議當事人處理事項（如變更密碼、信用卡停卡）、提供查詢及協助管道、補償當事人處理事務相關費用等補救措施。

前項通知指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。

三十一、重大資通安全事件通報及應變作業應依國家資通安全通報應變作業綱要及各機關處理資通安全事件危機通報緊急應變作業注意事項辦理。

#### **陸、委外監督及對外提供審查**

三十二、研擬業務委外招標文件時，應評估廠商應具備個人資料保護管理能力，視實際需要於招標文件訂定評選項目或於採購契約訂定監督事項及罰則條款，本要點應列入採購契約文件供廠商遵循。

三十三、各組室於履約期間應定期確認廠商執行個人資料保護措施並予以記錄。

三十四、契約終止、解除或屆滿時，廠商應返還或刪除所保有之個人資料，或交接本局指定之其他單位，刪除存取權限，並切結未以任何形式保留備份或影本；續約廠商不在此限。

履約期間廠商員工離職或留職停薪，應說明所負責系統之存取權限及完成鎖定帳號或停止系統權限之時點，並應更換離職或留職停薪員工曾接觸之密碼。

三十五、依政府資訊公開法申請提供政府資訊，如涉及個人資料，除有本法第十六條但書情形外，應依政府資訊公開法第十八條第一項第六款不予提供或經去識別化後提供；議員索取資料者亦同。

#### 柒、保存期間及刪除

三十六、各組室應查明蒐集或處理個人資料適用法令所訂定之保存期間，未明定者，視執行業務必要性及合理性，於年度檔案分類及保存年限表明定或訂定經告知當事人之合理保存期間。

三十七、特定目的消失或保存期間屆滿時，應視個人資料載體性質為適當之刪除或停止處理、利用。

三十八、個人資料刪除或停止處理、利用前應對相關系統或服務作影響評估並妥為因應。

三十九、個人資料刪除作業得參考機關檔案保存年限及銷毀辦法、電子檔案銷毀作業指引及臺北市政府公務機密維護作業規定辦理。

四十、個人資料刪除後應檢查資料無法還原或再組合。

#### 捌、個人資料保護管理執行小組及專人

四十一、個人資料保護管理執行小組由本局主管會報成員及專人共同組成，任務如下：

- (一) 本局個人資料保護政策之擬議。
- (二) 本局個人資料管理制度之推展。
- (三) 本局個人資料風險之評估及管理。
- (四) 本局職員工之個人資料保護意識提升及教育訓練計畫之擬議。
- (五) 本局個人資料管理制度基礎設施之評估。
- (六) 本局個人資料管理制度適法性與合宜性之檢視、審議及評估。
- (七) 其他本局個人資料保護、管理之規劃事項。

四十二、本局專人辦理下列事項：

- (一) 當事人依本法第十條及第十一條第一項至第四項所定請求之考核。
- (二) 本法第十一條第五項及第十二條所定通知之考核。
- (三) 本法第十七條所定公開或供公眾查閱。
- (四) 本法第十八條所定個人資料檔案安全維護之考核。
- (五) 依本要點第四十一點第一項第四款所為擬議之執行。
- (六) 個人資料保護法令之諮詢。
- (七) 個人資料保護事項之協調聯繫。

- (八) 本局個人資料損害預防及危機處理應變之考核。
- (九) 本局個人資料保護方針及政策之執行。
- (十) 本局個人資料保護管理規劃。

**玖、附則**

- 四十三、遇有疑義者，應向專人洽詢或確認，必要時得提請個人資料保護管理執行小組研議。
- 四十四、因應法令修訂、技術發展或強化人格權保障，得為必要之補充及調整，並適時修正本要點。