

# 個人資料保護法施行細則

第一條 本細則依個人資料保護法（以下簡稱本法）第五十五條規定訂定之。

第二條 本法所稱個人，指現生存之自然人。

第三條 本法第二條第一款所稱得以間接方式識別，指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。

第四條 本法第二條第一款所稱病歷之個人資料，指醫療法第六十七條第二項所列之各款資料。

本法第二條第一款所稱醫療之個人資料，指病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方、用藥、施術或處置所產生之個人資料。

本法第二條第一款所稱基因之個人資料，指由人體一段去氧核糖核酸構成，為人體控制特定功能之遺傳單位訊息。

本法第二條第一款所稱性生活之個人資料，指性取向或性慣行之個人資料。

本法第二條第一款所稱健康檢查之個人資料，指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料。

本法第二條第一款所稱犯罪前科之個人資料，指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄。

第五條 本法第二條第二款所定個人資料檔案，包括備份檔案。

第六條 本法第二條第四款所稱刪除，指使已儲存之個人資料自個人資料檔案中消失。

本法第二條第四款所稱內部傳送，指公務機關或非公務機關本身內部之資料傳送。

第七條 受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之。

第八條 委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。

前項監督至少應包含下列事項：

- 一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。
- 二、受託者就第十二條第二項採取之措施。
- 三、有複委託者，其約定之受託者。
- 四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。
- 五、委託機關如對受託者有保留指示者，其保留指示之事項。
- 六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。

第一項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。

受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。

第九條 本法第六條第一項第一款、第八條第二項第一款、第十六條第一項第一款、第十九條第一項第一款、第二十條第一項第一款所稱法律，指法律或法律具體明確授權之法規命令。

第十條 本法第六條第一項第二款、第八條第二項第二款及第三款、第十四條第二款、第十五條第一款、第十六條所稱法定職務，指於下列法規中所定公務機關之職務：

- 一、法律、法律授權之命令。
- 二、自治條例。
- 三、法律或自治條例授權之自治規則。
- 四、法律或中央法規授權之委辦規則。

第十一條 本法第六條第一項第二款、第八條第二項第二款所稱法定義務，

指非公務機關依法律或法律具體明確授權之法規命令所定之義務。

#### 第十二條

本法第六條第一項第二款所稱適當安全維護措施、第十八條所稱安全維護事項、第二十七條第一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。

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。

#### 第十三條

本法第六條第一項第三款、第九條第二項第二款、第十九條第一項第三款所稱當事人自行公開之個人資料，指當事人自行對不特定人或特定多數人揭露其個人資料。

本法第六條第一項第三款、第九條第二項第二款、第十九條第一項第三款所稱已合法公開之個人資料，指依法律或法律具體明確授權之法規命令所公示、公告或以其他合法方式公開之個人資料。

#### 第十四條

本法第七條所定書面意思表示之方式，依電子簽章法之規定，得以電子文件為之。

#### 第十五條

本法第七條第二項所定單獨所為之書面意思表示，如係與其他意思表示於同一書面為之者，蒐集者應於適當位置使當事人得以知悉其

內容並確認同意。

第十六條 依本法第八條、第九條及第五十四條所定告知之方式，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。

第十七條 本法第九條第二項第四款、第十六條但書第五款、第十九條第一項第四款及第二十條第一項但書第五款所稱資料經過處理後或依其揭露方式無從識別特定當事人，指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人。

第十八條 本法第十條第三款所稱妨害第三人之重大利益，指有害於第三人個人之生命、身體、自由、財產或其他重大利益。

第十九條 當事人依本法第十一條第一項規定向公務機關或非公務機關請求更正或補充其個人資料時，應為適當之釋明。

第二十條 本法第十一條第三項所稱特定目的消失，指下列各款情形之一：  
一、公務機關經裁撤或改組而無承受業務機關。  
二、非公務機關歇業、解散而無承受機關，或所營事業營業項目變更而與原蒐集目的不符。  
三、特定目的已達成而無繼續處理或利用之必要。  
四、其他事由足認該特定目的已無法達成或不存在。

第二十一條 有下列各款情形之一者，屬於本法第十一條第三項但書所定因執行職務或業務所必須：  
一、有法令規定或契約約定之保存期限。  
二、有理由足認刪除將侵害當事人值得保護之利益。  
三、其他不能刪除之正當事由。

第二十二條 本法第十二條所稱適當方式通知，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。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。

依本法第十二條規定通知當事人，其內容應包括個人資料被侵害

之事實及已採取之因應措施。

第二十三條 公務機關依本法第十七條規定為公開，應於建立個人資料檔案後一個月內為之；變更時，亦同。公開方式應予以特定，並避免任意變更。

本法第十七條所稱其他適當方式，指利用政府公報、新聞紙、雜誌、電子報或其他可供公眾查閱之方式為公開。

第二十四條 公務機關保有個人資料檔案者，應訂定個人資料安全維護規定。

第二十五條 本法第十八條所稱專人，指具有管理及維護個人資料檔案之能力，且足以擔任機關之個人資料檔案安全維護經常性工作之人員。

公務機關為使專人具有辦理安全維護事項之能力，應辦理或使專人接受相關專業之教育訓練。

第二十六條 本法第十九條第一項第二款所定契約或類似契約之關係，不以本法修正施行後成立者為限。

第二十七條 本法第十九條第一項第二款所定契約關係，包括本約，及非公務機關與當事人間為履行該契約，所涉及必要第三人之接觸、磋商或聯繫行為及給付或向其為給付之行為。

本法第十九條第一項第二款所稱類似契約之關係，指下列情形之一者：

一、非公務機關與當事人間於契約成立前，為準備或商議訂立契約或為交易之目的，所進行之接觸或磋商行為。

二、契約因無效、撤銷、解除、終止而消滅或履行完成時，非公務機關與當事人為行使權利、履行義務，或確保個人資料完整性之目的所為之連繫行為。

第二十八條 本法第十九條第一項第七款所稱一般可得之來源，指透過大眾傳播、網際網路、新聞、雜誌、政府公報及其他一般人可得知悉或接觸而取得個人資料之管道。

第二十九條 依本法第二十二條規定實施檢查時，應注意保守秘密及被檢查者之名譽。

第三十條 依本法第二十二條第二項規定，扣留或複製得沒入或可為證據之個人資料或其檔案時，應掣給收據，載明其名稱、數量、所有人、地點及時間。

依本法第二十二條第一項及第二項規定實施檢查後，應作成紀錄。

前項紀錄當場作成者，應使被檢查者閱覽及簽名，並即將副本交付被檢查者；其拒絕簽名者，應記明其事由。

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。

第三十一條 本法第五十二條第一項所稱之公益團體，指依民法或其他法律設立並具備個人資料保護專業能力之公益社團法人、財團法人及行政法人。

第三十二條 本法修正施行前已蒐集或處理由當事人提供之個人資料，於修正施行後，得繼續為處理及特定目的內之利用；其為特定目的外之利用者，應依本法修正施行後之規定為之。

第三十三條 本細則施行日期，由法務部定之。