個人資料事故通知通報及應變辦法草案總說明

「個人資料保護法」（以下簡稱本法）業於一百十四年十一月十一日修正公布，其施行日期由行政院定之。本法第十二條第四項明定，公務機關或非公務機關知悉所保有之個人資料被竊取、竄改、毀損、滅失或洩漏（以下簡稱個資事故）時，應通知或通報之內容、方式、時限與通報範圍、應變措施、紀錄保存及其他相關事項之辦法，由主管機關定之。為使公務機關或非公務機關於知悉個資事故時適時通知當事人、通報主管機關及採取即時有效之應變措施，俾使當事人得自主維護其權益、使主管機關掌握事態並按其影響程度進行適切之調查及協助，避免損害擴大、強化個資事故之監管，爰依前開規定訂定「個人資料事故通知通報及應變辦法」（以下簡稱本辦法）草案，其要點如下：

一、本辦法訂定之依據。（草案第一條）

二、個資事故通知當事人時限、方式及內容。（草案第二條）

三、個資事故通報時限、方式、範圍及內容。（草案第三條）

四、知悉個資事故後應採取之應變措施。（草案第四條）

五、委託關係之知悉時點。（草案第五條）

六、個資事故調查紀錄之應記載事項及保存期限。（草案第六條）

七、本辦法之施行日期。（草案第七條）

個人資料事故通知通報及應變辦法草案

條文	說明
第一條　本辦法依個人資料保護法（以下簡稱本法）第十二條第四項規定訂定之。	明定本辦法訂定之依據。
第二條　公務機關或非公務機關（以下簡稱事故機關）知悉所保有之個人資料被竊取、竄改、毀損、滅失或洩漏（以下簡稱個資事故），應於知悉時起七十二小時內以適當方式個別通知當事人。但有下列情形之一者，事故機關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，並應至少連續公開三十日： 一、未有個資事故所涉當事人之聯絡方式、聯絡方式有遺失或無法辨識之情事，致無法以適當方式個別通知當事人。 二、該個資事故未涉有本法第六條第一項所規定之個人資料，且該個人資料已經採取適當保護措施，致未經授權者無法讀取其內容。 三、所採個別通知當事人之方式需費過鉅，將影響事故機關之營運。 前項通知內容應包括下列事項： 一、發生個資事故時間及事實。 二、受影響之個人資料類別。 三、依第四條規定採取之應變措施。 四、事故機關聯絡方式、救濟或諮詢管道。	一、為使當事人儘速知悉個資事故，俾其有所警覺後，得自主評估、關注可能之權益損害，避免損害擴大，同時為利事故機關辦理通知之事項明確、一致，參考南韓個人資料保護法第三十四條、該法施行令第三十九條、日本個人資料保護法第二十六條及該法施行規則第九條規定，於第一項明定事故機關知悉個資事故後，應於七十二小時內以適當方式個別通知當事人。另符合特定情形時，事故機關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，例如事故機關若主張本條第一項第三款事由，應釋明個別通知當事人具體金額之計算方式，以及該金額何以影響營運之說明。 二、為利當事人得以確切掌握個資事故情形，以採取適當作為，保障其權益，爰於第二項明定通知內容應包括事項。 三、為使當事人得儘速知悉個資事故，於第三項明定事故機關通知當事人之適當方式。 四、考量個資事故樣態多元，爰於第四項明定事故機關倘未能於知悉起七

第一項所稱適當方式，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。 事故機關有正當事由未能於第一項所定期限內通知當事人者，應敘明具體事由送本法第十二條第二項受理通報之機關，並應於未能如期通知之事由消滅後七十二小時內依第一項規定補行通知。	十二小時內通知當事人者，應敘明具體事由送本法第十二條第二項受理通報之機關，惟仍應於未能如期通知之事由消滅後七十二小時內依第一項規定補行通知，以保障當事人權益。
第三條　個資事故屬下列通報範圍之一者，事故機關應於知悉時起七十二小時內依主管機關指定之方式向本法第十二條第二項所定機關辦理個資事故之通報： 一、涉有本法第六條第一項所規定之個人資料。 二、所涉之資通系統保有個人資料筆數達一萬筆以上。 三、所影響之個人資料筆數達一百筆以上。 前項通報內容應包括下列項目： 一、個資事故機關名稱。 二、個資事故發生時間及地點。 三、事故機關知悉個資事故時間及來源。 四、個資事故發生原因及類型。 五、個資事故所涉個人資料類別、估計數量及損害狀況。 六、依第二條規定通知當事人之方式及內容。 七、依第四條規定採取之應變措施。	一、為落實我國個人資料保護，參考南韓個人資料保護法第三十四條、該法施行令第四十條、日本個人資料保護法第二十六條、該法施行規則第七條、第八條及第四十三條規定，於第一項明定事故機關辦理個資事故通報之範圍。事故機關知悉屬應通報範圍者，應於知悉時起七十二小時內依主管機關指定之方式及對象辦理通報。又知悉起算點係以事故機關知悉個資事故且該個資事故符合第一項各款通報範圍時，開始起算七十二小時。另個人資料筆數之計算，比照個人資料檔案安全維護管理辦法第四條第一項規定，以非公務機關或公務機關單日所保有每一自然人之每一蒐集特定目的加總計算。 二、為強化個資事故之管理、追蹤及加速處理之效率，於第二項明定事故機關辦理個資事故通報作業之基本通報項目。

八、其他相關事項。 事故機關因故無法依第一項所定主管機關指定方式通報者，應於同項所定時間內依其他適當方式通報，並註記無法依主管機關指定方式通報之事由。 因天災、事變或其他不可抗力之事由，致事故機關不能於第一項所定期間內通報者，應於妨礙事由消滅後四十八小時內向本法第十二條第二項所定機關補行通報，並註記無法於第一項所定期間內通報之事由。	三、事故機關辦理通報時，倘發生無法依主管機關指定之方式進行個資事故通報之情事，例如事故機關所在地發生網路或電力中斷，致無法向主管機關所指定之個資事故通報網站辦理通報等情事，爰於第三項明定因故無法依指定方式通報時，事故機關應依其他適當方式進行通報，並註記說明阻礙通報之事由。 四、考量事故機關遇有天災、事變等情況危急之不可抗力事由，無法於第一項所定期間內通報個資事故時，為保護其生命、財產安全，同時兼顧個資事故之管理，爰於第四項明定事故機關仍應於妨礙事由消滅後四十八小時內補行通報。
第四條　事故機關知悉個資事故後，應採取下列即時有效之應變措施： 一、檢查洩漏途徑，並採取隔離或封鎖措施。 二、檢查存取權限，阻止異常存取路徑。 三、收回誤送之個人資料檔案；要求第三人刪除或銷毀誤送之個人資料檔案。 四、請求搜尋引擎業者刪除已公開之個人資料，或為消除該等個人資料公開狀態之措施。 五、其他即時有效防止個資事故擴大之措施。 事故機關辦理前項應變措施，應綜合考量個資事故之發生原因、受影	一、為保障個人資料當事人權益，避免個資事故可能產生之損害擴大，參考南韓個人資料保護法第三十四條規定及南韓個人資料委員會發布之個人資料外洩等事故應對手冊內容，於第一項明定事故機關於知悉個資事故後，應採取即時有效之應變措施。另隨著科技進步，駭客攻擊手法日新月異，爰於第五款明定事故機關得視個案情形，採取其他得即時有效防止個資事故擴大之應變措施。 二、考量導致個資事故發生之原因多元，事故機關所得採取避免損害擴大之手段不應僵化，宜視個案情形彈性調整，爰於第二項明定事故機關

響人數、個人資料類別及筆數、潛在風險等因素擇定之。	辦理應變措措施時，得綜合考量與事故有關之因素予以擇定。
第五條　受事故機關委託蒐集、處理及利用個人資料者，於本法適用範圍內知悉個資事故，視為委託機關知悉。 前項情形，受託者應於知悉個資事故時，立即通知事故機關並保存通知紀錄。	一、依本法第四條規定，受委託蒐集、處理及利用個人資料者，於本法適用範圍內，視同委託機關。同法施行細則第七條及第八條亦規範，受託者依委託機關適用之規定及委託機關對其負有監督義務。是以，受託者於本法適用範圍內知悉個資事故，視為委託機關知悉。 二、為使事故機關委託他人處理資料時之通報責任明確，參考歐盟一般資料保護規則（General Data Protection Regulation）第三十三條第二項規定，於第一項明定事故機關應於本法適用範圍內要求受託者應於知悉個資事故時，立即通知事故機關，同時明定受託者應保存通知紀錄，理屬當然。惟受託者違反第二項所定通知事故機關之義務，本法並無法對受託者裁罰；此時，事故機關除有行政罰法所定不予處罰之規定外（例如無故意或過失），以事故機關違反通知或通報義務之行為論處。至於受託者疏未通知，致事故機關遭行政裁罰，雙方關係應回歸委託契約或民法規定處理，併予敘明。
第六條　事故機關知悉個資事故後，應依本法第十二條第三項規定，以書面或電子方式製作相關紀錄，該紀錄應包括下列事項：	一、事故機關於知悉個資事故後，應妥為記錄對於個資事故之處理情形，以證明其於事故發生後善盡採行適當安全措施之義務，爰於本條明定

一、個資事故發生時間、地點及事故機關知悉個資事故時間、來源。 二、個資事故發生原因、所涉受影響當事人人數及個人資料類別、筆數。 三、依第二條規定通知當事人之情形。 四、依第三條規定通報之情形。 五、已採取即時有效防止損害擴大之應變措施及後續因應措施。 六、個資事故所生之影響。 七、調查方式、過程、結果及相關佐證資料。 八、倘有違反本辦法所定情事，經主管機關令限期改正，就改正措施之處置歷程及相關佐證資料。 前項相關紀錄，應於知悉個資事故之翌日起至少保存五年。但其他法規有較長之規定者，依其規定。	事故機關應製作相關紀錄及其應載事項。 二、鑑於個資事故通知當事人及通報主管機關之義務，均以知悉個資事故起算，爰明定個資事故相關紀錄應自該知悉個資事故之翌日起至少保存五年。
第七條　本辦法施行日期，由主管機關定之。	配合本法修正期程，明定施行日期由主管機關定之。