

立法院議案關係文書 (中華民國41年9月起編號)
中華民國112年3月22日印發

院總第 20 號 委員提案第 10032460 號

案由：本院委員王美惠、伍麗華 Saidhai Tahovecahe、許智傑等 25 人，鑑於近年個資外洩事件頻傳，如 2022 年 10 月傳出我國近 2,300 餘萬筆戶政資料遭販賣、2023 年健保資料遭健保署前主秘竊取、我國知名租車業者個資外洩案等，顯見無論是公家機關或私人企業，皆面臨著有心人士竊取個資的問題，乃至於遭國安單位認證已形成國際嚴重犯罪問題。為落實憲法所保障之隱私權、回應歐盟一般資料保護原則（General Data Protection Regulation, GDPR）精神，爰擬具「個人資料保護法部分條文修正草案」。是否有當？敬請公決。

說明：

- 一、對於同一原因事實造成超過一名當事人受到權力侵害之事件，經當事人請求損害賠償者，其合計最高總額原以新臺幣二億元為限。惟迄上次修正損害賠償總額上限已逾十二年，且近年科技發展快速，公務或非公務機關之發展已資訊化，各機關蒐集、處理、利用或國際傳輸個人資料之情形日益普遍。為督促個人資料蒐集及持有之公務及非公務應負有維護責任，提升損害賠償之最高總額實屬必要。
- 二、營利社團法人憑藉科技之進步，得以自身產品或服務，透過雲端、大數據、物聯網等科技應用成果，極易獲取大量個人資料。為避免上述資料受侵害，實應提升營利社團法人損害賠償最高總額之限制。且營利社團法人之規模大小與獲取之資料量應為正相關，故參照歐盟 GDPR 第八十三條之規定，增訂損害賠償最高總額亦得以前一會計年度全球年營業額之百分之二為上限，兩者取最高者為準。
- 三、現行違反本法第六條第一項、第十九條及第二十一條第一項，最高僅可處以新臺幣五十萬元罰鍰。惟企業大型資料庫進行資安維護、個資保護之成本，與現行罰則相比極度不符合比例原則，對於企業無嚇阻之效果，爰適當調高此項罰鍰至五百萬元。

立法院第 10 屆第 7 會期第 5 次會議議案關係文書

四、企業落實社會責任，個人資料安全之維護應為最低基本責任，若有觸犯者應給予罰鍰。惟現行裁罰金額過低，與企業進行資安維護之成本有極大之差距，故適當提高本條之罰鍰，以符合比例原則，更可促使企業落實完善資安之保護。

提案人：王美惠	伍麗華	Saidhai Tahovecahe	許智傑	
連署人：蔡易餘	賴惠員	林俊憲	湯蕙禎	莊瑞雄
何欣純	林宜瑾	陳素月	黃世杰	羅美玲
李昆澤	洪申翰	吳思瑤	吳玉琴	劉建國
張其祿	張宏陸	張廖萬堅	吳琪銘	黃秀芳
陳秀寶	陳明文			

個人資料保護法部分條文修正草案對照表

修正條文	現行條文	說明
<p>第二十八條 公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。</p> <p>被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。</p> <p>依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。</p> <p>對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣<u>三億元</u>為限。但因該原因事實所涉利益超過新臺幣<u>三億元</u>者，以該所涉利益為限。</p> <p>同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受第三項所定每人每一事件最低賠償金額新臺幣五百元之限制。</p> <p>第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。</p> <p><u>本條例中華民國○年○月○日修正之條文，自公布</u></p>	<p>第二十八條 公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。</p> <p>被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。</p> <p>依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。</p> <p>對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。</p> <p>同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受第三項所定每人每一事件最低賠償金額新臺幣五百元之限制。</p> <p>第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。</p>	<p>一、修正第四項之損害賠償總額上限為三億元。</p> <p>二、對於同一原因事實造成超過一名當事人受到權力侵害之事件，經當事人請求損害賠償者，其合計最高總額原以新臺幣二億元為限。惟迄上次修正損害賠償總額上限已逾十二年，且近年科技發展快速，公務或非公務機關之發展已資訊化，各機關蒐集、處理、利用或國際傳輸個人資料之情形日益普遍。為督促個人資料蒐集及持有之公務及非公務應負有維護責任，提升損害賠償之最高總額實屬必要。</p> <p>三、歐盟於民國一百零五年通過一般資料保護規則（GDPR），並於一百零七年五月二十五日正式施行，其針對數據全球化之現象，擴大法域適用範圍和增設多層次之權利義務規定。參酌 GDPR 第八十三條第四項罰鍰之金額規定，違 GDPR 規定者，最處以一千萬歐元之行政罰鍰（相當我國新台幣三億元以上），且現行條文對公務機關採幾近無過失責任，較 GDPR 嚴格，故僅以三億元為損害賠償最高總額之上限。</p> <p>四、增訂第七項，鑒於此罰鍰調升關資料安全維護、法規遵循等成本。為避免形成障礙，俟修正草案三讀通過並經總統同意公布後起一年施</p>

<p><u>日後一年施行。</u></p>		<p>行，俾利相關單位擬定相應計畫。</p>
<p>第二十九條 非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。</p> <p>依前項規定請求賠償者，適用前條<u>第三項</u>。係營利社團法人者，亦可以前一會計年度全球年營業額之百分之二為上限，兩者取較高者為準。</p> <p>依前項規定請求賠償者，適用前條<u>第二項、第四項至第七項</u>規定。</p>	<p>第二十九條 非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。</p> <p>依前項規定請求賠償者，適用前條<u>第二項至第六項</u>規定。</p>	<p>一、修正第二項。現行條文對非公務機關採舉證倒置責任，嚴格度與歐盟 GDPR 相同。又營利社團法人憑藉科技之進步，得以自身產品或服務，透過雲端、大數據、物聯網等科技應用成果，極易獲取大量個人資料。為避免上述資料受侵害，實應提升營利社團法人損害賠償最高總額之限制。且營利社團法人之規模大小與獲取之資料量應為正相關，故參照歐盟 GDPR 第八十三條之規定，增訂損害賠償最高總額亦得以前一會計年度全球年營業額之百分之二為上限，兩者取最高者為準。</p> <p>二、第三項為原條文第二項，為配合第二項之修正，移列至第三項。</p>
<p>第四十七條 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）政府處新臺幣五萬元以上五百萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之：</p> <p>一、違反第六條第一項規定。</p> <p>二、違反第十九條規定。</p> <p>三、違反第二十條第一項規定。</p> <p>四、違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或處分。</p>	<p>第四十七條 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）政府處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之：</p> <p>一、違反第六條第一項規定。</p> <p>二、違反第十九條規定。</p> <p>三、違反第二十條第一項規定。</p> <p>四、違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或處分。</p>	<p>現行違反本法第六條第一項「不得蒐集之特定個人資料」、第十九條及第二十一條第一項「非公務機關蒐集個資限制」，最高僅可處以新臺幣五十萬元罰鍰。惟企業大型資料庫進行資安維護、個資保護之成本，與現行罰則相比極度不符合比例原則，對於企業無嚇阻之效果。爰適當調高此項罰鍰至五百萬元，除以符合比例原則，更可促使企業落實完善資安之保護。</p>
<p>第四十八條 非公務機關有下列情事之一者，由中央目的</p>	<p>第四十八條 非公務機關有下列情事之一者，由中央目的</p>	<p>一、參酌各國違反個資安全維護義務的罰鍰，韓國針對業</p>

<p>事業主管機關或直轄市、縣（市）政府處新臺幣二萬元以上二百萬元以下罰鍰，<u>並命其限期改正，屆期未改正者，按次處二萬元以上一千元以下罰鍰</u>：</p> <p>一、違反第八條或第九條規定。</p> <p>二、違反第十條、第十一條、第十二條或第十三條規定。</p> <p>三、違反第二十條第二項或第三項規定。</p> <p>四、違反第二十七條第一項或未依第二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。</p>	<p>事業主管機關或直轄市、縣（市）政府<u>限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰</u>：</p> <p>一、違反第八條或第九條規定。</p> <p>二、違反第十條、第十一條、第十二條或第十三條規定。</p> <p>三、違反第二十條第二項或第三項規定。</p> <p>四、違反第二十七條第一項或未依第二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。</p>	<p>者最高罰鍰為四億韓元，約新臺幣八百六十四萬元；歐盟 GDPR 有企業之百分之二營業額或一千萬歐元之規定。顯見我國現行之處罰不符比例原則。</p> <p>二、企業落實社會責任，個人資料安全之維護應為最低基本責任，若有觸犯者應給予罰鍰。惟現行裁罰金額過低，與企業進行資安維護之成本有極大之差距，故適當提高本條之罰鍰，以符合比例原則，更可促使企業落實完善資安之保護。</p>
--	---	---

立法院第 10 屆第 7 會期第 5 次會議議案關係文書