

理律盃模擬法庭辯論賽研習營

個人資料保護基本原則

理律法律事務所

蕭秀玲律師

2022年9月17日



大綱

- 一、個人資料定義
- 二、個人資料保護基本原則
 - (一) 合法、公正、透明
 - (二) 目的限制
 - (三) 資料最小化
 - (四) 正確
 - (五) 儲存限制
 - (六) 完整和保密

個人資料定義



個人資料立法目的

保護個人 隱私權 ，避免人格權受侵害	促進個人資料合理利用
---------------------------	------------

資訊隱私權

憲法保障之基本權利

人民自由決定： ➤ 是否揭露 ➤ 在何種範圍、於何時、以何種方式、向何人揭露	➤ 事前控制：同意利用與否 ➤ 事後控制：請求刪除、停止或限制利用 <i>(111憲判13：健保資料)</i>
如何使用：知悉與控制權	
記載錯誤：更正權 <i>(釋603：指紋)</i>	

資訊隱私權

告知：資訊透明—蒐集哪些資料、目的、如何使用

蒐集：特定目的 + 告知後同意 or 其他法定事由

利用：特定目的外利用→新的同意

事後隨時瞭解、更正及撤回的權利

資訊隱私權：指紋

指紋乃重要個人資訊
個人對指紋資訊之自主控制，受資訊隱私權保障

國家得以法律**適當限制**

強制人民按捺指紋並予錄存，否則不發給身分證：

目的為何？戶籍法未設明文規定

→於憲法保障人民資訊隱私權之意旨未合

為身分證防偽、防止冒領、冒用，辨識路倒病人、迷途失智者、無名屍體等目的：

→損益失衡、手段過當，不符比例原則

基於特定**重大公益目的**而有**大規模蒐集、錄存人民指紋、建立資料庫儲存之必要**：

- 應以法律明定蒐集目的
- 蒐集應與**重大公益目的**之達成，具有密切必要性與關聯性
- 應明文禁止法定目的外使用
- 應配合當代科技發展，運用足以確保資訊正確及安全之方式，並對指紋檔案採取組織上與程序上必要之防護措施（**釋603**）

資訊隱私權：血液

血液乃屬高敏感個人生物資訊之重要載體

強制抽血檢測酒精濃度：

國家基於公益必要，非不得立法強制取得

- 取得與利用之目的、範圍與程序，應以法律明確規定；
 - 應依個人資訊屬性、取得方式、利用目的與範圍，設定相當之正當法律程序，以及確保資訊不受濫用與不當洩露之適當防護機制
- 憲法第23條法律保留原則，保障人民資訊隱私權

如依肇事現場客觀情況或肇事駕駛人身體外部狀況（身上存有酒氣）判斷，有相當理由可認係酒駕肇事，且情況急迫，有必要迅速保全酒駕證據→強制實施血液酒測為必要手段：

就憲法上特別重要公共利益維護，與肇事駕駛人之人身自由與身體權保障兩者間之損益，難謂失衡

可能因疲勞、分心、疏忽、躲避異物、車輛機械突然故障或路況不熟悉。如客觀上不具強制檢定體內酒精濃度值之合理性與必要性，就防制酒駕以確保交通與用路人安全之立法目的實現而言，難謂無其他替代可能性之必要手段，違反憲法第 23 條比例原則

(111 憲判1)

資訊隱私權：健保資料

個人健保資料包含高敏感特種個資，具高度個體差異，客觀上非無以極端方式還原而間接識別當事人之可能性，無論原始型態或經處理，均屬「得直接或間接識別該個人」之資料

→當事人對於此類資料之自主控制權，受憲法保障

公務機關或學術研究機構基於醫療、衛生之統計或學術研究目的，得於一定條件下強制蒐集、處理或利用個人健保資料：

- 毋須當事人同意，當事人大幅喪失自主控制權
- 應受法律明確性原則與比例原則之審查

個人健保資料可能描繪個人生活區域、**行動軌跡**，由病歷、醫療及健康檢查資料內所含之傷病與醫療處遇史，諸如職業傷病、家暴傷害或性犯罪傷害、罹病與投藥紀錄、手術與診療影像紀錄、家族高危險疾病因子、生育紀錄、疫苗接種紀錄，亦可能描繪**個人曾經歷之職業環境、社會生活事件、家庭與經濟環境、個人決策模式**等極私密敏感事項。

- 如受侵害，致生危害結果之嚴重性，尤甚於指紋
- 系爭規定是否合於比例原則，應採較指紋個資蒐集更高之嚴格標準審查
- 目的應係為追求特別重要之公益，手段應有助於目的之達成，且為最小侵害手段，所犧牲之私益與所追求之公益間應具相稱性 **(111憲判13)**

個人資料自主：禁止跟追

縱於**公共場域**，亦享有**不受持續**注視、監看、監聽、接近等侵擾的私人活動領域及個人資料自主

基於人性尊嚴理念，維護個人主體性及人格自由發展，亦屬憲法第22條保障之基本權利，不因身處**公共場域**，而失其必要性

無正當理由，**跟追他人**，經勸阻不聽，處罰鍰或申誡（社維法§89(2)）
尾隨、盯梢、守候或其他類似方式，持續接近他人，即時知悉他人行蹤，足以對他人身體、行動、私密領域或**個人資料自主**構成侵擾

禁止跟追他人或盯梢婦女

- 行動自由
- 身心安全
- **個人資料自主**
- 於公共場域不受侵擾之自由

合理隱私期待：

- 主觀期待
- 表現於外
- 依社會通念認為合理（**釋689**）

個人資料定義(1)

可識別當事人 (例示)

姓名、生日、
身分證、護照號碼、
特徵、**指紋**、
婚姻、家庭、
教育、職業、聯絡方式、財
務情況、社會活動§2

特種個人資料 (列舉)

病歷、醫療、基因、性生
活、健康檢查、犯罪前科
§6

透過網路IP、瀏覽紀錄產
生之數位軌跡

個人資料定義(2)

直接識別

間接識別

僅以該資料不能識別，須與其他資料對照、組合、連結等，始能識別特定個人。
~~但查詢困難、需耗費過鉅或耗時過久始能特定者，不在此限。~~
~~施行細則修正草案說明：如查詢有困難、需耗費過鉅或耗時過久始能特定者，屬技術上太複雜及經濟上不可行，應屬無法識別之個人資料，爰規定如但書條文，以資衡平個人資料保護與個人資料合理利用。（施§3）~~

無從識別

個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識特定個人（施§17）
公務或學術研究機構，基於公共利益，為統計或學術研究而有必要，資料經過提供者處理後或經蒐集者依其揭露方式，無從識別特定當事人§9、16、19、20

經處理後，客觀上仍有還原而間接識別當事人之可能，無論還原識別之方法難易，若以特定方法還原而可間接識別個人，仍屬個資（*111憲判13*）

完全匿名，**無還原可能性**→不在個資法保護範圍

去識別化：假名

無從識別當事人 (§6、9、16、19、20)

個人資料以代碼、匿名、隱藏部分資料或以其他方式，無從辨識特定個人 (施§17)

人體生物資料庫管理條例

<p>編碼： 以代碼取代參與者姓名、國民身分證統一編號、病歷號等可供辨識之個人資料，使達到難以辨識個人身分之作業方式</p>	<p>加密： 將足以辨識參與者個人身分之資料、訊息，轉化為無可辨識之過程</p>	<p>去連結： 於生物檢體、資料、資訊編碼後，使其與可供辨識參與者之個人資料、資訊，永久無法以任何方式連結、比對之作業</p>
--	--	--

假名化 (pseudonymization)：例如編碼，仍可透過與其他資料串連以識別個人。
匿名化 (anonymization)

去識別化：匿名

所謂「去識別化」，係指透過一定程序的加工處理，使個人資料不再具有直接或間接識別性而言（本部 107 年 4 月 26 日法律字第 10703505830 號函參照）。

本案民眾身分證照片倘依演算法轉換為不可逆之特徵值後，已無從直接或間接識別該特定個人者，即非屬個人資料，自非個資法之適用範圍。

法務部民國 107 年 08 月 30 日法律字第 10703513050 號函

個人資料保護基本原則

南韓重罰Google和Meta

蒐集用戶在其他平台的使用資訊，進行分析

- 推測用戶可能感興趣的資訊，據此投放個人化廣告
- 很難確認被搜集的行為資訊包含範圍，連動個人帳戶資訊，長久累積下來可能涉及敏感資訊

沒有明確告知

- 用戶只能利用一次只顯示5行的滾動式視窗，查看694行的隱私政策

沒有提供自由選擇權=沒有取得同意

- 將隱私政策選項設定為「默認同意」
- 僅將相關條文放在「看更多選項」當作基本條文一併同意。
- 用戶不同意蒐集資訊，即無法利用部分服務

2022.09.14



(一) 合法、公正、透明

lawfulness, fairness and transparency



透明原則：告知義務(1)

直接蒐集	間接蒐集
機關名稱	
蒐集目的	
資料類別	
利用期間、地區、對象、方式	
當事人權利及行使方式	
不提供對當事人權益影響	資料來源

透明原則：告知義務(2)

直接蒐集§8	間接蒐集§9
向當事人蒐集個人資料時告知	第一次接觸當事人時告知

明確告知

個別告知，不得以公告取代

不限書面

不得強制當事人簽署確認書或同意書

合法原則：蒐集、處理法定事由

特種個資§6	一般個資§15	一般個資§19
法律明文		法律明文
執行法定職務或義務必要範圍+安全維護	執行法定職務必要範圍	契約或類似契約+安全維護
自行or合法公開		自行or合法公開
基於醫療、衛生或犯罪預防目的，為統計或學術研究，資料 無從識別特定當事人		基於公共利益，為統計或學術研究，資料 無從識別特定當事人
當事人書面同意	當事人同意	當事人同意
為協助執行法定職務或義務+安全維護		增進公共利益必要
		一般可得來源*
	對當事人權益無侵害	對當事人權益無侵害

*須衡量當事人是否顯有更值得保護之重大利益

非基於當事人同意的蒐集

資訊隱私權之保障核心在於保護個人對資料之自主控制權
個資之蒐集、處理及利用，應以取得**當事人同意**為原則

基於其他事由**強制**蒐集、處理及利用個資，本庭於審查時，應視個資屬性及其對隱私之重要性，採不同寬嚴之審查標準，以定其是否合於**比例原則**。

§6 I(4) 就原則禁止蒐集、處理或利用之高敏感特種個資，例外容許**公務機關或學術研究機構**基於**醫療、衛生法定目的之統計或學術研究必要**，且擬蒐集、處理或利用之資料經一定程序處理後或揭露時，**無從識別特定當事人**之前提下，得未經當事人同意予以**強制**蒐集、處理或利用。

- 自行蒐集、處理與**原始利用**，就他人提供資料**延伸利用**，均毋須當事人同意。
- 當事人**大幅喪失**對其個人健保資料之**自主控制權**，構成對當事人受憲法第22條保障之**資訊隱私權之限制**，應受**法律明確性原則**與**比例原則**之審查。

指紋個資之蒐集：因指紋屬具備高度人別辨識功能之個資，居於開啟完整個人檔案鎖鑰之地位，採取**中度**審查（目的應為重大公益，手段應為與目的間具備密切關聯之**侵害較小**手段；釋603）

個人健保資料如受侵害，危害結果之嚴重性尤甚於指紋，應採較指紋個資蒐集更高之**嚴格**標準審查：目的應為追求特別重要之公益，手段應有助於目的達成，且為**最小侵害**手段，所犧牲之私益與所追求之公益間應具相稱性（111憲判13）

事前控制權：當事人同意

充分告知當事人本法所定應告知事項後，取得的同意

推定同意：

- 明確告知
- 當事人未表示拒絕
- 當事人已提供個資

蒐集者
負舉證責任§7

知情同意

蒐集通訊內容，改善服務

很少消費者閱讀隱私權政策

閱讀後無法完全理解：

- 冗長
- 手機畫面小
- 不會操作超連結

使用=預設同意？

繼續使用=喪失合理隱私期待？

透明的數位人

→行為模式受人為操控，逐漸麻痺，喪失自主決定能力

推定同意

公務機關或非公務機關 已明確告知	當事人未表示拒絕	當事人已提供個人資料
<p>服務延伸蒐集新的個資： 應依§8履行告知義務</p> <p>斟酌個案情形， 運用各種技術， 以簡化或便利方式通知 當事人。</p> <p>例如：以超連結顯示先 前已告知內容，由當事 人自行點選檢視。</p>	<p>在正面選擇同意與否的 模式下進行</p> <p>不得預設同意。</p>	<p>有自行提供的積極行為</p> <p>例如：自主開啟藍芽設 定，選擇同步定位資訊， 並將資料傳送業者。</p> <p>預設自動上傳資料功能， 不得視為當事人以提供 個人資料。</p>

(國發會發法字第1072002136號)

契約關係與推定同意

基於契約關係蒐集個資，僅能於**契約事務之特定目的**必要範圍內為之

蒐集**與契約履行無關**之個人資料或並非為履行契約所必需者，應另行取得當事人同意

有個資法第19條第1項第2款關係存在時，應優先適用此款，不能再以同條項第5款作為蒐集事由

- 避免當事人立於**不對等地位**而無法真正作成自主決定（例如：以同意做為契約成立前提）；甚至在已有其他合法事由下，仍尋求當事人同意，更有可能**顯失公平**。
- 若僅欲運用個資法第7條第3項**推定**「個資法第19條第1項第5款當事人**同意**」以規避個資法第20條第1項第6款特定目的外利用之規定，自非妥適。

行銷**與契約或類似契約內容無涉**之商品或服務資訊→特定目的外利用

行銷**合作或業務往來之關係企業及合作廠商之商品或服務**→將客戶個資提供當事人以外第三人，為特定目的外之利用

自行公開與合法公開(I)

自行公開	合法公開
對不特定人揭露	依法令公示或公告
對特定多數人揭露	以其他合法方式公開

喪失合理隱私期待？

自行公開與合法公開(2)

公開

秘密

當事人自行公開的個資

其他已合法公開的個資

§9免為告知

§6蒐集處理敏感個資

§19蒐集處理一般個資

喪失隱私權合理期待？



自行公開與合法公開(3)

董事長在夫人座車安裝GPS跟蹤

GPS衛星定位器所回傳小客車所在位置、動靜行止等資訊，是否係刑法第315條之1第2款「非公開活動」要件規範之範圍？

「非公開之活動」，包含公共場域之隱私活動
(臺高院106年度上訴字第3311號刑事判決)

個人之私人生活及社會活動，隨時受他人持續注視、監看、監聽或公開揭露，其言行舉止及人際互動即難自由從事，**致影響人格自由發展**。

尤以現今資訊科技高度發展及相關設備之方便取得，個人之私人活動受注視、監看、監聽或公開揭露等侵擾之可能大為增加，個人之私人活動及隱私受保護之需要，亦隨之提升。

自行公開與合法公開(4)

董事長在夫人座車安裝GPS跟蹤

個人縱於公共場域中，亦應享有依社會通念得不受他人『持續』注視、監看、監聽、接近等侵擾之私人活動領域及個人資料自主，而受法律所保護。

惟在公共場域中個人所得主張不受此等侵擾之自由，以得合理期待於他人者為限，亦即不僅其不受侵擾之期待已表現於外，且該期待須依社會通念認為合理者（司法院釋字第689號解釋理由書參照）。

車輛使用人行駛於道路或其他公共場域，固係處於同時間利用同一空間之他人可得共見共聞之狀態。惟他人之私密領域及個人資料自主，如在公共場域受到干擾，而超出可容忍之範圍，該干擾行為亦有加以限制之必要，俾有不受他人持續追蹤及侵擾之私人活動領域，而得保有「**獨處之權利**」。

自行公開與合法公開(5)

董事長在夫人座車安裝GPS跟蹤

車輛在公共道路上之行跡，伴隨駕駛或乘員即時發生之活動行止，除明示放棄隱私期待之情形（例如：公共汽車或計程車於車身上標示駕駛人之姓名、保全從業人員駕駛公司裝設衛星追蹤器之車輛執行業務），通常可認其期待**隱沒於道路上之往來車輛，不欲公開其個人行蹤**。倘若汽車駕駛人駕車行駛於供公眾往來道路上，而無以特別之方式引起他人注視，其亦非公眾人物或基於公益事由而有行蹤為眾人週知之必要，應可認其主觀上不欲公開其個人行蹤，且汽機車經由車廂或頭戴安全帽與外界隔離，一同利用該公共道路之其他人車通常不易察覺該駕駛或乘員之身分，而能自在的選擇移動方向、路徑、速度以及停止地點，客觀上自無須採取其他確保活動隱密性之舉止。

經由衛星追蹤器即時紀錄車輛之動態行止及狀態，可以連結至駕駛或乘員之行蹤，仍與個人即時之隱私活動密切相關，並不當然排除在刑法第315條之1所保護對象之外。

自行公開與合法公開(6)

董事長在夫人座車安裝GPS跟蹤

以GPS定位追蹤器可**連續多日、全天候不間斷**追蹤他人車輛行駛路徑及停止地點，將可鉅細靡遺長期掌握他人行蹤，此等**看似瑣碎、微不足道**之活動資訊，經由此種「拖網式監控」大量地蒐集、比對定位資料，個別活動之**積累集合**將產生內在關連，使以此等方式取得之資料**呈現寬廣的視角場景**，私人行蹤將因此被迫揭露其**不為人知之私人生活圖像**。

質言之，**經由長期大量比對、整合**車輛行跡，該車輛駕駛人之慣用路線、行車速度、停車地點、滯留時間等活動將可一覽無遺，並可藉此探知車輛使用人之日常作息、生活細節及行為模式。此一經由科技設備對他人進行長期且密集之資訊監視與紀錄，他人**身體在形式上雖為獨處狀態，但心理上保有隱私之獨處狀態已遭破壞殆盡**，自屬侵害他人欲保有隱私權之非公開活動。

自行公開與合法公開(7)

政府使用GPS進行犯罪偵查

行車路徑是否為**公開**個資，當事人不具合理隱私期待？

是否能**合理預期**公開場所活動會被政府全面記錄，瞭解、推估個人的家庭、政治、專業、信仰、性關係的細節？

公開場合**單一**時點**單一**行為，可能無法享有隱私權保護。

每一時點每個**單一**行為都被詳細記錄，串連成**行動軌跡**，經由分析，即足以整合出不是在公開場合**單一**時點**單一**行為所能顯示的隱私內涵。

自行公開與合法公開(8)

司法陽光網

整合分析司法官資料

巨量個資的組合使用

馬賽克理論：量變產生質變

→整合眾多單筆個資，透過統計分析，
產生大於單筆個資相加的效果

當事人對個別公開的個資，不具有合理隱私期待。

當各筆分別公開的個資被組合使用，受到無法合理預見的隱私傷害

(二) 目的限制 purpose limitation



利用個資

一般個資 16 執行法定職務必要範圍+特定目的	一般個資 20 特定目的的必要範圍
有下列情形，可以為特定目的外利用：	
法律明文	法律明文
國家安全 or 公共利益必要	公共利益必要
免除生命、身體、自由、財產危險	免除生命、身體、自由、財產危險
防止他人權益重大危害	防止他人權益重大危害
基於公共利益，為統計或學術研究， 資料 無從識別特定當事人	基於公共利益，為統計或學術研究， 資料 無從識別特定當事人
有利於當事人權益	有利於當事人權益
當事人同意	當事人同意

特定目的外利用的同意

充分告知：

- 其他利用目的
- 範圍
- 權益影響

單獨意思表示：

- (x) 與其他事項不當聯結
- (x) 列入定型化契約概括同意

同一書面：

適當位置
知悉內容
+
確認同意

當事人同意

蒐集時告知，取得同意

資訊透明

資訊控制權

無限授權？

同意時無法合理預期的利用

特定目的外利用
的同意

公共利益

去識別化

巨量資料(1)

蒐集大量和多樣化的資料
因應**無法預期**的使用

透過大規模分析，產出新型態資料
特定目的外利用

巨量資料(2)

Google流感預測

Google蒐集用戶搜尋的關鍵字。

目的：改善搜尋引擎效果

蒐集發燒喉嚨痛等關鍵字

目的：預測某地區流感爆發的可能性

→ 特定目的外利用：當事人同意？

隱私保護v.公共利益

事後控制權：可否撤回同意？

個資法第16條第5款規定及第20條第1項第5款規定，「公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人」時，公務機關或非公務機關得為特定目的外之利用，且該案個人資料如係公務機關或非公務機關基於本法第15條第2款及第19條第1項第5款（當事人書面同意）以外之要件而蒐集者，其利用之範圍則非當事人所得限制。惟公務機關或非公務機關為利用時，自仍應符合本法第5條規定。

個人資料者，乃涉及當事人之隱私權益，故本法立法目的之一乃在個人人格權中隱私權之保護。準此，依本法第16條第5款或第20條第1項第5款規定，用於統計或學術研究之個人資料，經提供者處理後或蒐集者依其揭露方式無從再識別特定當事人，則該筆經提供者處理後之資料或蒐集者揭露之資料已非本法第2條第1款所定「得以直接或間接方式識別該個人之資料」，即無本法之適用。

法務部民國101年7月30日法律字第10103106010號書函

事後控制權：請求刪除、停止利用

倘業者基於當事人同意蒐集、處理個人資料，而當事人事後撤回同意，則自撤回時起，如蒐集個人資料之特定目的或要件已不存在，除有上開個資法第11條第3項但書規定之情形外，業者應主動或依當事人之請求，刪除、停止處理或利用該等個人資料（法務部106年11月10日法律字第10603512680號書函）

- 資訊隱私權：保障當事人就其個資受利用之前，有同意利用與否之**事前控制權**，以及受利用中、後之**事後控制權**。
- 當事人就**獲其同意**或符合特定要件而允許**未獲當事人同意**而經蒐集、處理及利用之個資，**仍具事後控制權**。
- 事後控制權之內涵：包括請求刪除、停止利用或限制利用個資之權利（111憲判13）

健保資料

將**強制蒐集**之個人健保資料建立成資料庫，作原始蒐集**目的外利用**
基於醫療、衛生之統計及學術研究目的
尚難謂不符**特別重要公益目的**之標準

但，應由**獨立監督機制**，依申請個案之相關情狀作嚴格審查

確保已逸脫個人控制範圍之個人健保資料，不受濫用或不當洩漏，導致資訊隱私權之侵害繼續擴大，**國家有義務**以法律積極建置適當之**組織與程序性防護機制**，以符法律保留原則之意旨

- 此一限制個人資訊隱私權之行為，當事人之**停止利用權**仍受憲法第22條規定保障。
- 由相關法制整體觀察，未見立法者依所保護個人資訊隱私權與利用目的間法益輕重及手段之必要性，而為適當權衡及區分。
- 欠缺**當事人得請求停止利用**之相關規定，於個人資訊隱私權之保護有所不足，違反憲法第22條保障人民**資訊隱私權**之意旨（111憲判13）

(三) 資料最小化 data minimisation



目的限縮，資料最小化

尊重當事人權益

依誠實信用方法

不得逾越特定目的**必要範圍**

與蒐集目的具有**正當合理關聯**§5



健保資料

§6 I(4)課予提供者採取去識別化措施之義務

- 一般人採取當時存在技術與合理成本，在不使用額外資訊時，不能識別特定當事人。
- 雖個人健保資料於客觀上非無以極端方式還原而間接識別特定當事人之可能性，惟所採之去識別化手段已足大幅降低蒐用個人健保資料所生之個人資訊隱私權所生之侵害。

與個人資訊隱私權之最小蒐用原則尚屬相符

- 明定目的限於醫療、衛生（排除其他目的）
- 蒐用主體以公務機關及學術研究機構為限（排除其他人），
- 以統計或學術研究且必要→排除非為統計或學術研究者，暨非必要之統計及學術研究

去識別化資料：最小侵害手段

匿名資料固非全然不具學術研究價值，但已喪失病歷、醫療、基因及健康檢查資料作為學術研究樣本時可擇定變因交互比對、建立相關性之特性，無從達成系爭規定所欲追求之特別重要公益目的（111憲判13）

酒測檢體

授權採檢範圍，除血液外，尚及於「**其他檢體**之採樣及測試檢定」

即便技術上可從血液以外之檢體（如尿液或其他身體組織）驗出酒精反應，亦無從據以判定是否酒駕，難以成為酒駕處罰之證據。
→ **逾越**駕駛人應配合警察所實施之酒精濃度測試檢定之義務範圍，亦**非有效**取得肇事駕駛人體內酒精濃度值之**適合手段**。

手段無助立法目的實現，**非**別無其他替代可能性之**最小侵害手段**
遑論對肇事駕駛人身體權之**侵犯顯然過度**而有失均衡
明顯違反憲法第23條比例原則之要求（**111憲判1**）

(四) 正確
accuracy



維護資料正確

- 主動或依當事人請求，更正或補充
- 正確性有爭議：停止處理或利用
- 例外：
 - 當事人書面同意
 - 執行職務或業務所必須（並註明爭議）

有法令規定或契約
約定之保存期限

有理由足認刪除將侵害
當事人值得保護之利益

其他不能刪除之
正當事由

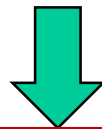
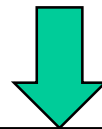
- 應於更正或補充後，通知曾提供利用之對象(§11)

(五) 儲存限制 storage limitation



資料保存及刪除

- 個資法沒有規定保存年限
- 安全維護措施：使用紀錄、軌跡資料及證據的保存
- 蒐集特定目的消失、期限屆滿：應主動或依當事人請求，刪除、停止處理或利用
- 例外：執行職務或業務所必須或經當事人書面同意
- 特定目的消失：



裁撤、改組、歇業、解散，沒有承受業務機關

營業項目變更，與原蒐集目的不符

目的已達成，無繼續處理或利用之必要

其他事由足認目的已無法達成或不存在

當事人權利：不得限制

- 查詢及閱覽
- 複製
- 補充及更正
- 停止處理或利用
- 刪除

➡ 不得預先拋棄、不得以契約限制§3

當事人權利：可否拒絕？

拒絕查詢、閱覽、複製

- 妨害國家安全、外交及軍事機密、整體經濟利益、國家重大利益
- 妨害公務機關執行法定職務
- 妨害蒐集機關或第三人重大利益 §10

拒絕刪除、停止處理利用

- 正確性無爭議
- 特定目的未消失
- 期限未屆滿
- 執行職務或業務必須
- 當事人書面同意 §11



(六) 完整和保密

integrity and confidentiality



維護資料安全

手段	目的
<ul style="list-style-type: none">• 指定專人辦理安全維護事項§18• 採行適當安全措施§27• 個人資料安全維護計畫• 業務終止後個人資料處理方法 <p><u>技術上措施</u></p> <ul style="list-style-type: none">• 上鎖、加密、保全或防護設備 <p><u>組織上措施</u></p> <ul style="list-style-type: none">• 人員、流程、存取權限、教育訓練	防止個人資料被竊取、竄改、毀損、滅失或洩漏

符合比例原則的安全措施

配置管理人員及相當資源：隱私長(CPO) 任命及權責

界定個資範圍

風險評估、管理機制

事故預防、通報及應變機制

內部管理程序

資安管理、人員管理

認知宣導、教育訓練

設備安全管理

資安稽核

使用紀錄、軌跡資料及證據保存

安全維護整體持續改善（施§12）

組織和程序上必要之防護措施

保障資訊隱私權

- 以法律明確訂定蒐用個資之**目的及要件**
- 配合當代科技發展，運用足以確保**資訊正確及安全**之方式
- 採取**組織上與程序上必要之防護措施**（釋603）。

個資保護之獨立監督機制為重要之關鍵制度

- 獨立監督機制之目的：確保個資蒐用，符合法令規定，以增強個資蒐用之**合法性與可信度**
- 尤其個人健保資料已逸脫個人控制範圍，如何避免**不受濫用**或**不當洩漏**，更有賴獨立機制之監督（*111憲判13*）

個資外洩通知當事人之義務

- 違法致個資被竊取、洩漏、竄改、有其他侵害情形

查明事實

採取因應措施

通知當事人

- 個別通知
- 網際網路、新聞媒體、其他適當公開方式

敬請指教

蕭秀玲律師
理律法律事務所
11072台北市忠孝東路四段555號8樓
話：886-2-27638000 分機 2257
傳真：886-2-27665566
電子郵件：rebeccaHSiao@leeandli.com

