《2021 行政管制與行政爭訟》　王必芳主編
臺北　中央研究院法律學研究所　法學叢書 (8)
民國 114 年 7 月，頁 231-280



# 基於防疫目的之預防性個人資料運用*
## —— 以實聯制為例

李寧修**

## 摘　要

2019年底，全球陸續爆發嚴重特殊傳染性肺炎（以下簡稱COVID-19）疫情，各國面對此一公共衛生緊急事件，皆採行了不同之手段及措施，企圖阻斷疫情之蔓延。其中，國家藉由蒐集、處理及利用個人資料，進行分析並應用於COVID-19防治之作法，時有所聞，本文將擇其中基於防疫目的而實施之實聯制為例，其藉由預先蒐集、處理及利用人民之個人資料，以利未來用於回溯追蹤足跡，釐清感染源並防阻疫情擴散。此一措施，立意固然良善，惟在保障人民資訊隱私權之觀點下，其是否已完備所應遵循之基本法制框架？透過對實聯制實施依據、要件及運作模式之分析，歸納其於個人資料蒐集、處理及利用上可能衍生之相關爭議，並同時觀察德

---

＊　本文曾刊載於公法研究，創刊號，頁113-152（2022年）。
〔責任校對：蕭惟文、楊子萱〕。
本文首次發表於「2021行政管制與行政爭訟」學術研討會——防疫與法治，感謝主持人劉淑範老師、與談人邱文聰老師給予之寶貴意見，以及二位匿名審查人關鍵性地提點與建議，讓本文得以更為完整周延，敬謹致謝，惟文責仍應自負。本文係執行科技部補助專題研究計畫「警察職權行使與個人資料保護之研究：以歐盟、德國及臺灣法制之比較為重心（MOST 110-2423-H-034-001-MY4）」之部分研究成果，對於計畫執行提供諸多協助之研究助理施孝儀先生，於此一併表達感謝之意。另，隨著疫情起伏，法規變動亦相當頻繁，本文內容及相關數據僅相應關注至2022年3月28日，合先敘明。

＊＊ 中國文化大學法律學系教授。
穩定網址：https://publication.iias.sinica.edu.tw/70901042.pdf。

國法制與實務之運作，提出個人之觀察及建議，期得對未來我國傳染病防治法制與實務之發展與精進，盡棉薄之力。

關鍵詞：個人資料、資訊隱私權、COVID-19、實聯制、傳染病防治法、個人資料保護法。

**目　次**



## 壹、前言

2019年底，全球陸續爆發嚴重特殊傳染性肺炎（以下簡稱COVID-19）疫情，延燒至今，似仍方興未艾，隨著疫情發展詭譎多變，防疫措施亦是千變萬化，其中，國家藉由蒐集、處理及利用個人資料，進行分析並應用於COVID-19防治之作法，時有所聞，例如：對於確診者或高風險染疫者，進行疫調；運用電子圍籬系統，監控受隔離者或受檢疫者之行蹤；發送細胞簡訊，通知與確診者足跡有重疊之民眾；採行簡訊實聯制，以利未來回溯追蹤足跡等，皆為適例。但不論是何種防疫措施，皆是透過限制人民之自由

及權利，以求取公眾健康與安全之保護，然而，即便是基於重大公益目的之國家行為，仍應謹守法治國原則之要求。以實聯制為例，其即係於防疫過程中，藉由預防性地蒐集、處理及利用個人資料，用於未來回溯追蹤足跡，藉以釐清感染源並採行相應之措施，例如：要求與確診者曾有接觸之人，進行居家隔離或自主健康管理，以求有效防阻疫情擴散，其立意雖屬良善，然而，國家蒐集人民之足跡資料，對其受憲法保障之「個人自主控制個人資料之資訊隱私權」，自然將產生一定之干預，該權利雖非不得限制，然而，限制是否合乎比例？究竟該等個人資料被國家進行何種後續利用、利用之要件及範圍為何、人民對於利用之情形是否及從何知悉、是否有採行相關安全維護措施以確保資料之安全等議題，皆屬檢證國家是否遵循法治國要求時，不可忽略之重要面向。

首先，本文將就國家基於防疫目的，預先蒐集、處理及利用人民個人資料之行為，透過保障人民資訊隱私權之觀點，確認我國現行傳染病防治法及「『COVID-19（武漢肺炎）』防疫新生活運動：實聯制措施指引」（以下簡稱實聯制指引）所規範之實聯制法制架構；進而，聚焦我國之實聯制，分析其運作模式及可能衍生之相關爭議；最後，擬以德國在建構足跡追溯系統時，所使用之紙本表格及Luca App，及作為其法制基礎之德國傳染病防治相關法規及歐盟個人資料保護基本規則（Datenschutz-Grundverordnung, DSVGO）之適用模式，提出個人之觀察及建議，期得在我國實聯制法制框架之建構面，略盡棉薄之力。

# 貳、實聯制之法制框架

## 一、憲法層次之觀察：資訊隱私權之保障

資訊隱私權雖未明列於我國基本權利清單中，但隨著司法院大法官解釋對於隱私權之闡述，其受憲法保障之脈絡亦逐漸清晰：「隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障。」個人資料自主控制之資訊隱私權，係屬隱私權所保障之範疇，受憲法第22條保障，藉以「保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。[1]」

隨著科技日新月異的發展，如何保障個人自主控制個人資料之權利，更顯其重要性，「蓋隨電腦處理資訊技術的發達，過去所無法處理之零碎、片段、無意義的個人資料，在現今即能快速地彼此串連、比對歸檔與系統化。當大量關乎個人但看似中性無害的資訊

1 司法院釋字第603號解釋參照。其中對於個人自主控制個人資料權利之論述，不難發現德國聯邦憲法法院長期透過相關判決所闡明之資訊自決權概念，對於我國釋憲實務所帶來的顯著影響：德國資訊自決權得溯及至1983年之人口普查判決中，德國聯邦憲法法院引用德國基本法第2條第1項之一般人格權，併同第1條第1項人性尊嚴觀察，而得出其之保障內涵：「自決權的概念乃是賦予個人就何時、於何種界限內公開其個人生活的內涵，享有自我決定的權限」、「在現代資料處理之條件下，應保護每個人之個人資料免於遭受無限制之蒐集、儲存、運用、傳遞，……。該基本人權保障原則上每個人有權自行決定其個人資料之交付與使用。」而「在一個法律秩序中，人民若無法知道其個人資料被何人所知悉、何以被知悉、為何被知悉、以及在何種機會下被知悉，則此一社會秩序及其所賴以存在之法律秩序，將與資訊自決權之意旨未盡合致。」Vgl. BVerfGE 65, 1 (42 ff.). 上述中譯請參考Christian Starck著，李建良譯，基本權利之保護義務，收於：法學、憲法法院審判權與基本權利，頁425-426（2006年）；西德聯邦憲法法院著，蕭文生譯，關於「一九八三年人口普查法」之判決，收於：西德聯邦憲法法院裁判選輯（一），頁288以下（1990年）。

累積在一起時，個人長期的行動軌跡便呼之欲出。誰掌握了這些技術與資訊，便掌握了監看他人的權力。[2]」當網路及行動上網裝置逐漸普及，每個人所遺留下的數位足跡，不論是在監視器中的身影、手機傳送至基地臺之訊號，或是查詢移動路線時所留下的定位，在透過與其他資料之結合、比對，皆提供了識別特定個人身分、行為、移動軌跡等之絕佳素材，若經長時間之蒐集與分析，甚至可能得以預測該特定人之慣用路線、消費習慣、社交喜好等，讓每個人的行為模式都無所遁形[3]。

由權利主體的角度觀察，每個人對於其本身或與其本身相關之資訊，無論是否涉及私密資訊，皆應得依其個人意志，為消極不提供或是積極公開之行為決定；對於被揭露之資訊，有權知悉並掌握其使用的歷程，即便是已獲同意並公開之資訊亦同；進而，對於資料的完整與正確性，人民得要求更正或更新；若國家運用個人資料的行為致生人民損害，則應設計相應之救濟途徑[4]。

而自國家的層面切入，在維護人民資訊隱私權之前提下，國家蒐集資訊之目的，應明確於事前以法律制定，讓人民對於其個人資料之利用得有預見可能性；此一目的同時拘束國家使用人民個人資訊之方式與範圍，確保其正當地使用該等資訊；另外，國家負有維護資訊安全之義務，並應建置相關管道讓資訊主體得知悉資訊之使

2 司法院釋字第603號解釋林子儀大法官所提出協同意見書參照。

3 關於數位時代中之個人資料保護，請參考林其樺，數位時代個人隱私界線怎麼畫？——從美國Carpenter v. United States案淺介行動電話定位資訊之隱私合理期待，科技法律透析，30卷11期，頁15（2018年）；郭戎晉，論數位環境下個人資料保護法制之發展與難題——以「數位足跡」之評價為核心，科技法律透析，24卷4期，頁27-28（2012年）；李建良，在瘟疫中思索自由，人文與社會科學簡訊，22卷1期，頁32（2020年）。

4 黃昭元，無指紋則無身分證？：換發國民身分證與強制全民捺指紋的憲法爭議分析，收於：國際刑法學會臺灣分會編，民主、人權、正義：蘇俊雄教授七秩華誕祝壽論文集，頁471-472（2005年）；李寧修，預防性通信資料存取之憲法界限——以歐盟儲備性資料存取指令（2006/24/EG）之發展為借鏡，興大法學，17期，頁100-101（2015年）。

用及處理情形；對於違法揭露個人資料的行為，國家自應承擔相關責任[5]。

惟「憲法對個人資訊隱私權之保護亦非絕對，國家基於公益之必要，自得於不違反憲法第二十三條之範圍內，以法律明確規定強制取得所必要之個人資訊。至該法律是否符合憲法第二十三條之規定，則應就國家蒐集、利用、揭露個人資訊所能獲得之公益與對資訊隱私之主體所構成之侵害，通盤衡酌考量。[6]」因此，在對抗COVID-19期間，對人民之資訊隱私權可能造成干預之措施，例如：於健保卡中註記旅遊史，並向醫療院所揭露特定地區14日內及30日內旅遊史[7]；針對受隔離或檢疫而有違反隔離或檢疫命令或有違反之虞者，公布其個人資料[8]，均應是在權衡防疫措施所欲維護之公眾生命及健康以及資訊隱私權後，所加諸之限制，在防疫如同作戰之情境中，人民或許「從善如流」，然而，當戰情暫歇，該措施是否仍有持續之必要性？若有轉為常態之規劃，則該措施之法制架構，應即回歸法治國原則下所要求之法律保留之層級、法律明確

5 關於國家運用個人資料應遵循之原則，請參考李震山，論國家機關蒐集資訊之合法性，收於：國立政治大學傳播學院研究暨發展中心、理律法律事務所編，傳播與法律系列研討會（七）論文彙編：監聽法vs.隱私權——全民公敵？，頁10-15（2001年）。

6 司法院釋字第603號解釋理由書第9段參照。

7 衛生福利部中央健康保險署，特定地區旅遊及接觸史VPN查詢作業，即日起開放非健保特約醫事服務機構申請，2020年2月19日，https://www.mohw.gov.tw/cp-16-51604-1.html（最後瀏覽日：2024年11月3日）；何建志，COVID-19疫情期間防疫與隱私之平衡：相關法律議題分析與社會正義觀點，台灣法學雜誌，387期，頁25-26（2020年）。

8 嚴重特殊傳染性肺炎防治及紓困振興特別條例第8條第1項（已於2023年7月1日廢止）：「於防疫期間，受隔離或檢疫而有違反隔離或檢疫命令或有違反之虞者，中央流行疫情指揮中心指揮官得指示對其實施錄影、攝影、公布其個人資料或為其他必要之防治控制措施或處置。」針對公布個人資料可能衍生之爭議，請參考何建志（註7），頁27-29；吳采模、高塚真希，「嚴重特殊傳染性肺炎防治及紓困振興特別條例」之概要及其法律問題，萬國法律，231期，頁112-113（2020年）；陳玥汝，我國紓困條例所涉隱私議題初探，科技法律透析，32卷5期，頁30-31（2020年）；林欣柔，防疫？妨疫？疾病監測、接觸者追蹤與個人資訊隱私之平衡，台灣法學雜誌，387期，頁50-51（2020年）。

性、比例原則、目的拘束原則等要求，以確保人民基本權利之保障，乃屬當然[9]。

## 二、現行規範架構

衛生福利部（以下簡稱衛福部）實於2020年5月間即已訂頒實聯制指引，其係考量國內疫情漸受穩定控制，為使民眾生活及產業經濟能逐步恢復正常運作，而以實聯制作為逐步開放過程中之配套措施。惟時至2021年5月中，因應COVID-19疫情警戒標準提升至三級警戒，衛福部依傳染病防治法第37條第1項第6款及同條第3項[10]，於2021年5月28日公告修正「嚴重特殊傳染性肺炎（COVID-19）第三級疫情警戒標準及防疫措施裁罰規定」[11]，明定「**外出時應全程佩戴口罩，並配合實聯制**」，將實聯制納入三級警戒之防疫措施，並強化執行。若有拒絕、規避或妨礙，依據傳染病防治法第70條第1項第3款之規定，處新臺幣3千元以上1萬5千元以下罰鍰；必要時，並得限期令其改善，屆期未改善者，按次處罰之[12]。

---

9 李崇僖，在瘟疫蔓延中檢視個資保護法制，台灣法學雜誌，387期，頁41-42（2020年）。

10 傳染病防治法第37條規定：「地方主管機關於傳染病發生或有發生之虞時，應視實際需要，會同有關機關（構），採行下列措施：
一、管制上課、集會、宴會或其他團體活動。
二、管制特定場所之出入及容納人數。
三、管制特定區域之交通。
四、撤離特定場所或區域之人員。
五、限制或禁止傳染病或疑似傳染病病人搭乘大眾運輸工具或出入特定場所。
六、其他經各級政府機關公告之防疫措施。
各機關（構）、團體、事業及人員對於前項措施，不得拒絕、規避或妨礙。
第一項地方主管機關應採行之措施，於中央流行疫情指揮中心成立期間，應依指揮官之指示辦理。」

11 衛福部於2021年5月28日公告修正「嚴重特殊傳染性肺炎（COVID-19）第三級疫情警戒標準及防疫措施裁罰規定」（2021年7月27日停用），衛福部網站，https://www.cdc.gov.tw/Uploads/archives/9f054c94-924f-418a-a5f4-6facfdf25456.pdf（最後瀏覽日：2024年11月3日）。

12 傳染病防治法第70條第1項規定：「有下列情事之一者，處新臺幣三千元以上一

COVID-19疫情警戒標準於2021年7月27日調降為二級，至今不論是面對疫情升溫，或是朝向逐步解封的過程中，均不難看出實聯制作為防疫措施，仍相當受到倚重[13]，另，於各主管機關修正或發布之眾多防疫管理指引中，亦得見應持續採行實聯制之要求[14]，頗有「預先準備，以防不時之需」之態勢。

觀察實聯制指引之規範內容，可概分為告知內容、資料安全維護義務、應採行資訊安全風險評估之情形、保存期間及刪除義務以及監督等五大部分，以下分別說明其所規範之內容，並就與其相關之個人資料保護法規定，併予說明。

---

萬五千元以下罰鍰；必要時，並得限期令其改善，屆期未改善者，按次處罰之：

一、違反第二十五條第二項規定。

二、拒絕、規避或妨礙主管機關依第三十六條規定所定檢查、治療或其他防疫、檢疫措施。

三、拒絕、規避或妨礙各級政府機關依第三十七條第一項第六款規定所定之防疫措施。

四、違反第四十六條第二項檢體及其檢出病原體之保存規定者。」

13 隨著疫情警戒降為二級，衛福部於2021年7月29日公告修正「嚴重特殊傳染性肺炎（COVID-19）第二級疫情警戒標準及防疫措施裁罰規定」，並同時自2021年7月27日起，停止2021年5月28日公告之適用，然而，觀察於此之後衛福部所公告之疫情警戒標準及防疫措施裁罰規定（直至現行有效之2022年3月28日發布之公告），相同之實聯制要求，並未曾改變。

14 以經濟部訂定之「會議及展覽防疫管理措施指引」為例，其針對會展活動期間，要求「確實執行分區實聯制：展館場地應分區並進行實聯制，另主辦單位應於會展活動之入口處／報到處設置掃瞄QR Code簡訊實聯制設施，確實掌握進入會展活動現場人員名單（包括從業人員、承包廠商、參展商、買主及參加者等），以利後續疫調聯繫，所蒐集之個資為配合中央疫情指揮中心疫調需求（保存28日後即銷毀），禁止目的外使用，並確保個資安全不外洩。（詳情請參閱中央疫情指揮中心公告之『實聯制措施指引』）」；而會展活動後，則應「協助中央單位疫情調查：應隨時配合衛福部、中央流行疫情指揮中心及地方政府衛生局之要求，提供實聯制資料及其他潛在接觸者之聯繫方式並協助追蹤。若有承包廠商、參展廠商及參加者等有疑似COVID-19感染，應儘速提供其他潛在接觸者之聯繫方式並協助追蹤，以協助疫情調查並控制。」

（一）告知內容

實聯制指引第2點要求蒐集機關於蒐集民眾個人資料時，應明確告知下列事項：

－蒐集機關之名稱。
－蒐集之目的：防疫目的，依據「個人資料保護法之特定目的及個人資料之類別」為代號012公共衛生或傳染病防治之特定目的，且不得為目的外利用。
－蒐集之個人資料項目：蒐集資料應符合最少侵害原則，如電話號碼。
－個人資料利用之期間：自蒐集日起28日內。
－個人資料利用之對象及方式：為防堵疫情而有必要時，得提供衛生主管機關依傳染病防治法等規定進行疫情調查及聯繫使用。
－當事人就其個人資料得依個人資料保護法規定，向蒐集之機關行使權利，包括查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止處理或利用、請求刪除，及行使方式。
－當事人不同意提供個人資料對其權益之影響，如無法進入場館或參與活動。

前述告知之內容，應係本於個人資料保護法第8條第1項就直接蒐集個人資料時應履行之告知義務[15]，而為相應之設計，藉此強化

15 個人資料保護法第8條第1項：「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：
一、公務機關或非公務機關名稱。
二、蒐集之目的。
三、個人資料之類別。
四、個人資料利用之期間、地區、對象及方式。
五、當事人依第三條規定得行使之權利及方式。
六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。」

防疫措施之透明性，以及提高民眾之信賴為目的，但考量告知事項之呈現可能較為龐雜，故實聯制指引中亦建議蒐集機關於告知時，可採取「多層次告知」方式，將重要事項於明顯處揭示，並以QR Code或網址連結提供其他細節事項，供民眾進一步查詢。

實聯制指引明確要求除防疫目的外，不得為目的外利用，且應限於達成目的所必要之範圍內為之，並符合最小侵害原則，因此，應以留存實際上得聯絡上當事人之方式為主；觀諸個人資料保護法第16條及第20條中，雖有關於在蒐集特定目的外利用之要件，但其於此應均無適用餘地，藉由遵循嚴格之「目的拘束原則」，提高民眾配合意願，以及宣示國家不會濫用實聯制資料之決心。惟於尊重當事人對其個人資料自主控制權之前提下，目的外利用若為基於「當事人同意」（個人資料保護法第16條第7款及第20條第1項第6款），是否仍應禁止目的外利用，則容有討論之空間。

實聯制之實施，對於民眾而言，雖非絕對強制，但不配合實聯制，確實將可能為其帶來負面之效果，例如：無法進入特定場域、無法參與活動或課程等，因此，實聯制指引要求針對當事人不同意提供個人資料對其權益之影響，應於蒐集時一併告知。然而，該告知並未包括，若民眾對於該權益之影響有所不服，是否得提出救濟，以及應如何及向何機關提出救濟之教示。

### （二）資料安全維護義務

實聯制指引第3點規定，個人資料之蒐集、處理及利用，得以紙本或電子方式為之，蒐集機關皆應善盡資料安全維護義務，採行適當之技術上及組織上安全措施，並指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏，例如：以紙本供當事人填具個人資料時，應以遮蔽或其他適當方式保護填寫者之個人資料，避免後填寫者得閱覽先填寫者之個人資料。

上述資料安全維護義務，與個人資料保護法課予公務機關（個人資料保護法第18條）及非公務機關（個人資料保護法第27條）之資料安全維護義務，應可為相同理解。參照個人資料保護法施行細則第12條第2項對於適當之安全措施，得包括之事項有：配置管理之人員及相當資源，界定個人資料之範圍，個人資料之風險評估及管理機制，事故之預防、通報及應變機制，個人資料蒐集、處理及利用之內部管理程序，資料安全管理及人員管理，認知宣導及教育訓練，設備安全管理，資料安全稽核機制，使用紀錄、軌跡資料及證據保存以及個人資料安全維護之整體持續改善[16]。並要求所採取之技術上及組織上措施，仍應與所欲達成之個人資料保護目的間，具有適當比例為原則。

### （三）應採行資訊安全風險評估之情形

所謂的風險評估，應是立基於一般人民對於科學根據的信賴，以獨立、客觀、透明的方式對風險進行評價。透過風險評估，以科學之觀點衡量危害或是風險的規模及強度，進而由預防原則出發，預先發現可能對當事人之權利產生風險的因素，提供是否需預先採行抑制或保護措施之決策參考。依據實聯制指引第4點，機關以資訊系統或App實施實聯制者，應進行資訊安全風險評估，採行相符安全控制措施，確保系統安全防護水準。

我國個人資料保護法雖尚未將個人資料之事前風險結果評估，納入蒐集、處理及利用個人資料之要件中，但參考法務部訂定之「公務機關執行個人資料保護法之參考事項」中，得見針對公務機關於其個人資料保護之規劃中，亦已置入對於個人資料採行風險評估之建議，包括就登載之個人資料檔案公開項目彙整表中之個人資料及各作業流程，分析可能產生之風險，並根據風險分析之結果，

16 何念修，個資保護「適當之安全措施」——以新加坡個資法之技術措施建議為比較對象，科技法律透析，31卷1期，頁60-61（2019年）。

訂定適當之管控措施；並為維持個人資料風險評估為最新之狀態，應定期檢視其更新狀況；另，「103年政府機關（構）資通安全稽核相關建議參考事項」中，亦明列下列參考事項：「1. 雖已進行個資盤點，但未定期進行後續之風險評估、衝擊分析及管理機制。2. 風險評鑑方式應適切反應資安與個資風險。3. 為定期進行個資風險評估、衝擊分析，建議能將所有個人資料周延納入，定期檢討分析，依不同個資類型或來源，予以檢視，俾充分發揮其功能。4. 於個資風險評鑑中，宜訂定風險門檻值，以決定可接受之風險，後續每年應賡續滾動檢討。5. 針對個資風險評估之結果，宜確認是否已採行適當之控制措施。」值得參考[17]。

與本文所欲探討之實聯制不同，但值得同時關注者為，衛福部疾病管制署（以下簡稱疾管署）、行政院資通安全處與臺灣人工智慧實驗室（Taiwan AI Labs）於2020年4月共同開發之科技防疫軟體「臺灣社交距離App」[18]，其係利用手持裝置的藍牙（Bluetooth）訊號強度，偵測使用者間接觸的距離與時間，記錄接觸對象去識別化資料，不包括地點定位資訊，相關接觸資料將儲存於個人手持裝置端14天，不會上傳到任何雲端服務。而當用戶接獲通知為確診者時，徵得其同意後，衛生主管機關可上傳資料，App將主動通知過去14天曾接觸過的對象（例如：曾與確診者於2公尺內接觸2分鐘以上者），並出現警示畫面，提醒用戶注意最近的身體狀況，藉以減少疫情擴散機會。因其係透過App蒐集並保存藍牙訊號間之接觸紀錄，並保留其14天內之可回溯性，惟其主要係幫助個人監測其自主

17 李寧修，個人資料合理利用模式之探析：以健康資料之學術研究為例，臺大法學論叢，49卷1期，頁41（2020年）。

18 衛生福利部疾病管制署，「臺灣社交距離App」已上架　鼓勵全民下載使用 掌握疫情擴散相關資訊，2021年5月14日，https://www.cdc.gov.tw/Bulletin/Detail/4tvSn4wPDjJe42YTuS8LjA?typeid=9（最後瀏覽日：2024年11月3日）。關於臺灣社交距離App之運作方式，請參考張陳弘，科技智慧防疫與個人資料保護：陌生但關鍵的資料保護影響評估程序，臺大法學論叢，50卷2期，頁343-347（2021年）。

健康，不論是下載App、開啟藍牙功能、通報衛生主管機關確診、回報接觸史等，皆有賴民眾自主決定是否配合，囿於此性質，其由外部追溯足跡，實際聯繫以提升疫調完整及正確性之功能恐亦將受限，故並非本文所欲討論之實聯制範圍，但即使其非屬實聯制指引所稱「以資訊系統或App實施實聯制者」，但是否應進行資訊安全風險評估，採行與系統安全防護水準相符之安全控制措施，應有進一步探究之空間[19]。

（四）保存期限及刪除義務

個人資料之保存，應訂定期限，當已達成目的或其對於目的達成不再有所助益時，即課予持有機關將其刪除或銷毀之義務，其係考量一旦欠缺刪除或銷毀之壓力，加以現今儲存技術便捷且成本低廉，恐會導向「永久保存」以備「不時之需」的結果，故個人資料法制中，普遍定有保存期限，以防免不合比例地利用個人資料之情形[20]。觀諸個人資料保護法之規定，其於第11條第3項中針對個人資料蒐集之特定目的消失或期限屆滿時，要求公務機關或非公務機關應主動刪除個人資料；或當事人依據個人資料保護法第3條第5款，得請求公務機關或非公務機關刪除其個人資料，藉由給予當事人相應之退場機制，以落實個人資料自主之權利，但針對執行職務或業務所必須或經當事人書面同意者，則不在此限，惟若以「執行職務所必須」作為豁免刪除義務之要件，其「必要性」仍應逐案認定，而不宜一概全面永久保存。觀諸實聯制指引第5點，明定各機關對於蒐集之個人資料僅可保存28日，屆期即應主動將個人資料予以刪除或銷毀，並應留存執行刪除或銷毀之項目及日期等軌跡紀

19 有強烈建議應採行如同歐盟個人資料基本保護規則第35條所要求之資料保護影響評估，並擬具詳細評估面向者，張陳弘（註18），頁367-371。

20 例如：警察職權行使法第10條第2項針對依據同條第1項以攝影、科技工具或裝設監視器所蒐集之資料，要求「除因調查犯罪嫌疑或其他違法行為，有保存之必要者外，至遲應於資料製作完成時起一年內銷毀之。」

錄。此以兩個潛伏期計算得出之28日保存期限，並於期限屆至後，課予持有資料機關主動刪除義務，與個人資料保護法之要求應屬相符，亦值得肯定。

（五）監督

各中央目的事業主管機關、直轄市、縣（市）政府應依個人資料保護法第22條規定，監督所轄非公務機關，落實執行上開個人資料保護事項，以兼顧民眾資訊隱私權之保障。

由實聯制指引所規範內容可知，蒐集機關於執行實聯制之過程，實被課予相當多樣之責任及義務。因此，除透過各中央目的事業主管機關、直轄市、縣（市）政府，確保遵法外，或可同時強化蒐集機關之內控機制：針對公務機關，依據個人資料保護法第18條：「公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏」之規定，應得要求指定專人負責實聯制相關事務；非公務機關部分，除得透過其中央目的事業主管機關依據個人資料保護法第27條第2項授權訂定之個人資料檔案安全維護計畫，給予與公務機關相同之要求外，或亦得依據個人資料保護法施行細則第12條第2項第1款：「配置管理之人員及相當資源」，強化非公務機關本身之內控機制。

## 參、實聯制之運作模式

所謂實聯制，即實際聯絡制，我國現行所採實聯制均屬分散式之建置模式，並未設置資訊系統或資料庫集中儲存所有實聯制之資料；亦未要求必須以特定、統一之方式實施，而是由有採行實聯制需求之公務機關或非公務機關，各自依其偏好選擇一或多種方式執行之。以下將擇三種目前較為常見之實聯制類型，說明其運作模式。

## 一、類型概分

### （一）紙本實聯制

第一種類型為紙本之形式，請民眾填具COVID-19防疫實聯制登記表留下相關資訊，其應填寫欄位包括：主要聯絡人、聯繫方式（如：手機或電話）、日期及時間、同行人數（含本人）、欲使用場地。登記表中並記載有下列告知事項：

－依據「個人資料保護法之特定目的及個人資料之類別」代號012公共衛生或傳染病防治之特定目的，蒐集以上個人資料，且不得為目的外利用。所蒐集之資料僅保存28日，屆期銷毀。

－個人資料利用之對象及方式：為防堵疫情而有必要時，得提供衛生主管機關依傳染病防治法等規定進行疫情調查及聯繫使用。

－當事人就其個人資料得依個人資料保護法規定，向○○○（資料蒐集機關）行使權利，包括查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止處理或利用、請求刪除等。相關權利行使方式：【例如】本人攜帶身分證明文件至（地址○○○）臨櫃申辦、或至（網址https://○○○）線上填具資料申辦。

－當事人如無法配合本實聯制作業，將○○○（請說明對其權益之影響，如無法進入場館或參與活動等）。

－本實聯制其他相關措施說明，請參閱http://at.cdc.tw/8QI4hA。

## 表1 因應「COVID-19」防疫新生活運動實聯制登記表（民眾自填版）

日期： 年 月 日 **民眾自填版**

**（場館名稱）**

**因應「COVID-19（武漢肺炎）」防疫新生活運動實聯制登記表（範本）**

| | |
|---|---|
| 時間（例：14:00） | |
| 1 位主要聯絡人（例：王先生） | |
| 聯繫方式（例：手機、家用或公司電話…） | |
| 同行人數（主要聯絡人於 28 天內須能聯絡同行所有人） | |
| 欲使用場地（例：○○室、○○場、○○廳、○○桌…） | |
| 備註（特殊事項紀錄說明） | |

備註：

1. 為維持國內疫情之穩定控制，本場所配合政府「COVID19（武漢肺炎）」防疫新生活運動，採行實聯制措施。依據「個人資料保護法之特定目的及個人資料之類別」代號012公共衛生或傳染病防治之特定目的，蒐集以上個人資料，且不得為目的外利用。所蒐集之資料僅保存28日，屆期銷毀。感謝您的配合。
2. 個人資料利用之對象及方式：為防堵疫情而有必要時，得提供衛生主管機關依傳染病防治法等規定進行疫情調查及聯繫使用。
3. 當事人就其個人資料得依個人資料保護法規定，向○○○○○（資料蒐集機關）行使權利，包括查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止處理或利用、請求刪除等。相關權利行使方式：【例如】本人攜帶身分證明文件至（地址○○○○○）臨櫃申辦、或至（網址 https://○○○○○）線上填具資料申辦。
4. 當事人如無法配合本實聯制作業，將○○○○○（請說明對其權益之影響，如無法進入場館或參與活動等）。
5. 本實聯制其他相關措施說明，請參閱 http://at.cdc.tw/8QI4hA。

資料來源：衛生福利部疾病管制署[21]。

21 COVID-19防疫新生活運動：實聯制措施指引，實聯制登記表_民眾自填版（範本），https://www.cdc.gov.tw/Category/Page/vNnZ-o-dP6JmsXEIf2Ix8Q（最後瀏覽日：2022年3月28日）。

此一類型在使用時所留下之資料，蒐集機關必須留意遭他人閱覽、抄錄，故應避免採取共用表格，因此，相當多蒐集機關會將登記表製作成較小之「紙條」形式，方便民眾填寫後直接投遞在蒐集之容器中，但亦因受限於篇幅，告知事項多會被大幅壓縮，不易閱讀。民眾若對其所提供之實聯制資料，欲行使個人資料保護法第3條所定權利時，得直接依據告知事項中所載權利行使方式，向蒐集機關提出。由於紙本登記之方式使用門檻較低，無須手機、網路，仍有許多民眾偏好此種形式，故在實聯制之實施上，應有保留此種可能性供民眾選擇之必要。但若由實際應用層面觀察，機關透過紙本實聯制所蒐集之資料，若後續無轉換為電子檔案管理，未來在衛生主管機關有調取需求時，勢必將耗費較高成本查找、比對，是否緩不濟急，因而降低主管機關使用之意願，紙本實聯制後端應用之實效，仍有待觀察。

### （二）簡訊實聯制

第二種類型則是簡訊實聯制，簡訊實聯制係由使用人自主掃瞄QR Code後，發送簡訊至1922，完成實聯制之足跡登錄，減少實聯制紙本填寫之接觸。而簡訊實聯制之資料並不會留存於採行實聯制之機關，其僅有在查核簡訊之過程中，可以目視確認場所代碼與簡訊送出之時間，實聯制之資料係傳送給電信業者，由其保留該活動史簡訊（包括手機號碼、手機號碼進入場所的時間與場所代碼）28天，該資料僅得供指揮中心疫調使用，禁止為目的外利用，且電信業者並未持有「場所代碼所對應的店家／場館」之資訊。

以目前普遍使用之行政院簡訊實聯制或臺北通App為例，二者皆是透過發送簡訊之方式達到實聯制之功能：前者於掃描QR Code後，將切換至「簡訊」，透過手機發送簡訊，所發送簡訊內容大致為：「場所代碼：〇〇〇本次實聯簡訊限防疫目的使用」，其強調免接觸、免App、免打字、免個資、免費，廣受歡迎，但在使用過程

中，實聯制指引所要求應明確告知之事項，卻似乎隱而不見；臺北通App在使用上則須先下載App，建立帳號完成註冊後方得使用，掃瞄QR Code，填寫同行人數後，必須在有網路連線支援之環境下進行通報，登記頁面中所顯示之注意事項如下：

「臺北市實聯（名）制系統即時將資料上傳並統一加密封存，超過疫調所需的28天後即刻刪除。民眾對個人資料保護將可更安心，也降低資安風險。

本次蒐集之個人資訊，僅限COVID-19（新冠肺炎）防疫措施應用之實聯（名）制系統使用，並遵守個人資料保護法相關規定，保障您的個資。請確認您填報的資料是否正確，並請提供服務人員查驗。點擊『確認登記』表示您同意完成此次填報。」

簡訊實聯制自2021年5月19日上線後，截至2022年3月27日已發送之簡訊實聯制數量，已累計達44億3,998萬1,288則，已刪除之數量則為41億4,665萬2,948則[22]。而自2021年同年6月3日啟用實聯制資料調用機制，提供地方衛生主管機關於有疫調需求時，得向中央流行疫情指揮中心（以下簡稱指揮中心）申請調閱，經審核通過後將調閱資料回覆，大多數申請調用案件可於1日之內提供資料。截至2021年6月29日，已有宜蘭縣、花蓮縣、南投縣、屏東縣、苗栗縣、桃園市、高雄市、基隆市、新北市、新竹縣、嘉義縣、彰化縣、臺中市、臺北市、臺南市、澎湖縣，共計16縣市政府衛生局調用303項資料，調用量前3名依序為桃園市衛生局、高雄市衛生局、臺中市衛生局[23]。另外，為落實「當事人就其個人資料得依個人資

22 關於目前已發送及已刪除之簡訊數量，請參考國家通訊傳播委員會，簡訊實聯制數量統計，2022年3月28日，https://www.facebook.com/1612318445669171/posts/pfbid0tWiPU9h85ss2Gd9KTTbg9rRuNt2Mtr4Znh3qWcrxcMS7vUvYfdXtWcW2B6mvDnWNl（最後瀏覽日：2024年11月3日）。

23 相關說明請參考衛生福利部疾病管制署，簡訊實聯制數據係以合法性、正當性、必要性進行使用，絕無違法情事，2021年6月29日，https://www.cdc.gov.tw/

料保護法規定，向蒐集之機關行使權利，包括查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止處理或利用、請求刪除，及行使方式」之要求，衛福部疾管署建置有「簡訊實聯制——民眾資料調閱紀錄查詢服務」[24]，民眾於該網頁中輸入手機號碼及驗證碼，並通過OTP身分驗證後，即得查詢過去28天之調閱紀錄，但該服務並無提供個人足跡紀錄之查詢。

### （三）實名制

第三種類型，則是透過留下實際身分資訊之方式為之，首先透過掃描QR Code或登入特定網路頁面，連結至特定頁面填寫表單（例如Google表單）後提交[25]，而於該表單中，「姓名」多為必填欄位之一，由於表單之設計可能因各單位而繁簡不一，但皆須一一輸入，較為耗時，故此種形式目前已較少見；另外，針對成員較為封閉之機關，如學校、公司，於掃瞄QR Code後，亦常見要求須先輸入個人資料，如：姓名、身分證字號、員工證號、學號等，方會出現准予通行之頁面，並記錄登錄者之身分、地點、日期與時間等資訊。

相較於前述實聯制，此類實名制特殊之處，在於蒐集資料階段，蒐集機關即已留存具有直接識別性之資料，或雖僅具間接識別性，但蒐集機關同時掌握有得對照、連結之關鍵性識別資料，例如：學籍資料庫、員工人事資料等；另外，針對所蒐集之足跡資料，與簡訊實聯制係集中傳送簡訊給1922，並由電信公司處理，實名制反倒是與紙本實聯制類似，係由蒐集機關保存於其自行或委託管理之資訊系統中。

---

Category/ListContent/EmXemht4IT-IRAPrAnyG9A?uaid=HS0hjvHxAOTCPtNPmDo7Bw（最後瀏覽日：2024年11月3日）。

24 衛生福利部疾病管制署所建置之「簡訊實聯制——民眾資料調閱紀錄查詢服務」網頁（https://sms.1922.gov.tw），現已關閉。

25 關於建立Google表單以落實實聯制之作法，請參考COVID-19防疫實聯制網站，https://sites.google.com/email.nchu.edu.tw/slimz/（最後瀏覽日：2024年11月3日）。

自從2021年5月19日行政院所推動之簡訊實聯制上線後，前述以填寫表單方式進行之實名制，實多已由簡訊實聯制取代；但在出入人員身分有特定性之機關，例如：學校，則多仍維持以此方式進行足跡資料之蒐集、處理。

然而，實聯制的採行，實不限於以上之形式，對於運用生物特徵辨識技術，精準記錄足跡之形式，不論是人臉辨識或指紋辨識系統，亦有所討論或應用[26]。但考量生物特徵資料性質敏感[27]，在蒐集、處理及利用之要件及程序配套上，皆應以較高之標準看待之。該等生物識別技術，實已廣泛被運用於身分識別之用途，例如：警察機關所配置之M-Police系統[28]、移民署之入出國自動查驗通關系統[29]或是許多門禁管控系統[30]，皆屬透過人臉辨識系統進行身分確認；而內政部警政署刑事警察局所建置之犯罪指紋資料庫及移民署針對外國人建置之入出境指紋資料庫，則是運用指紋辨識身分[31]。

---

26 落實實聯制！臺灣工研院創新AI熱影像體溫異常偵測技術結合門禁管制系統，台灣英文新聞，2021年6月21日，https://www.taiwannews.com.tw/ch/news/4228540（最後瀏覽日：2024年11月3日）。

27 針對指紋，大法官即曾於司法院釋字第603號解釋理由書第11段中指出：「指紋係個人身體之生物特徵，因其具有人各不同、終身不變之特質，故一旦與個人身分連結，即屬具備高度人別辨識功能之一種個人資訊。由於指紋觸碰留痕之特質，故經由建檔指紋之比對，將使指紋居於開啟完整個人檔案鎖鑰之地位。因指紋具上述諸種特性，故國家藉由身分確認而蒐集個人指紋並建檔管理者，足使指紋形成得以監控個人之敏感性資訊。」

28 請參考甘佳加，警察使用人臉辨識系統查證身分的合法性研究——以M-Police即時相片比對功能為中心，國立臺灣大學法律學研究所碩士論文（2021年）。

29 請參考李震山、許義寶、李寧修、陳正根、李錫棟、蔡庭榕、蔡政杰，入出國及移民法逐條釋義，2版，頁77-83（2024年）。

30 例如：由建碁智見股份有限公司所推出之「e臉通」，即為運用人臉辨識技術，進行非接觸式之門禁管理方式，提供100人內且單一出入口之門禁管理，系統功能包含：人臉識別、數位看板、員工管理與出勤管理等，並可搭配掌靜脈、紅外線體溫感測等非接觸性偵測功能。建碁智見股份有限公司，AI視覺技術偵測溫度、人臉及後台數據紀錄，企業防疫有效率，全球安防科技網，2020年4月14日，https://www.asmag.com.tw/suppliers/pressreleases.aspx?co=inferfy&id=3159（最後瀏覽日：2024年11月3日）。

31 蔡庭榕，我國與英國警察運用指紋個人識別載具適法性之比較分析，執法新知論衡，16卷2期，頁34-35（2020年）。

惟前述辨識身分目的之達成，除辨識技術之運用外，實有賴預先建立識別之基礎資料庫，若欲外加足跡追溯之功能，則該資料庫恐將難以避免「理所當然」地再與其他資料庫進行串連，例如：監視錄影器所攝錄畫面、入出境資料庫、全民健康保險資料庫、人事或出差勤資料等，相較於以紙本、簡訊甚至是以特定身分登入之實聯／名制，對於受蒐集者所造成之侵害顯然非屬較輕微，故以生物特徵輔助足跡紀錄之形式，在比例原則之考量下，恐不宜貿然採用。

## 二、可能之爭議

國家基於防疫目的，預防性蒐集、處理及利用人民之個人資料，在國家預防危害任務執行與人民自由權利保障間，確實可能會造成法益衝突與緊張關係，以下將針對現行實聯制可能產生爭議，提出初步之觀察。

防疫過程中之預防性資料存取，除係為預防危害發生而預先採行，考量防疫貴在迅速，往往需要主管機關於短時間作快速、專業之判斷並採行相應之因應措施，惟於事態之緊急程度降低，而措施仍須持續時，應即思考如何將其法制常態化，以法律明確規範，劃定權限行使之要件及範圍，並規劃行政及司法之監督予以把關，確保該職權行使之節制。若僅以實聯制指引作為實聯制運作之主要依據，是否妥適？對於指引之法律性質、效力及其所應遵循之程序，可能皆有進一步釐清之必要。

採行實聯制前所為告知，應屬強化防疫措施透明性之重要措施，亦可藉此強化蒐集人民個人資料之正當性，提高民眾之信賴，實聯制指引考量告知事項之呈現可能較為龐雜，故建議蒐集機關可採取「多層次告知」方式，將重要事項於明顯處揭示，並以QR Code或網址連結提供其他細節事項，供民眾進一步查詢，但是否有確切落實，不無疑義。告知之欠缺，將使人民無從掌握究竟哪些個

人資料在何時、何種情況之下、被誰、基於何種目的、為何種利用，其作為個人資料主體所得主張之任何權利，恐怕亦將落空。

司法院釋字第603號解釋曾闡明：「主管機關尤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為之，並對所蒐集之指紋檔案採取組織上與程序上必要之防護措施，以符憲法保障人民資訊隱私權之本旨。」於此基本權利逐漸相互衝突而需要平衡的時代，透過組織與程序之建構，應是緩解基本權利衝突之適切方法。加以實聯制指引所主張之「禁止目的外利用」、「28天後刪除」、「安全維護義務」等承諾，究竟是否有確實遵循，仍宜有相應監督機制之設計，包括救濟之可能性亦應一併納入思考[32]。惟目前我國個人資料保護法係採分散式管理，非公務機關部分係交由各目的事業主管機關監管；公務機關則依既有之行政監督權責為劃分，並暫由個人資料保護委員會籌備處擔任法律主管機關，主要著重於個人資料保護業務之協調與相關法規之統一適用，但此種監管型態，除欠缺個人資料保護監管機制中強調之獨立性，某種程度上，恐怕亦有弱化對公務機關自身監督之疑慮[33]。

---

32 例如：針對透過簡訊實聯制所保存之足跡，檢調機關是否得依據通訊保障及監察法，向法官申請通訊監察書，於經法官同意後，在通訊監察系統就該簡訊實聯制內容進行監察，值得探究，相關爭議請參考「行政命令、一般處分之法定程式及法制監督機制——防疫措施法制爭議」公聽會報告，立法院第10屆第4會期，頁34，陳明堂次長發言（2021年）。以及張淵森法官於天下雜誌獨立評論專欄之文章，張淵森，我必須成為吹哨者：「簡訊實聯制」資訊遭利用，指揮中心請儘速反應，天下雜誌獨立評論，2021年6月23日，https://opinion.cw.com.tw/blog/profile/509/article/11042（最後瀏覽日：2024年11月3日）；以及國家通訊傳播委員會公布之澄清新聞稿，國家通訊傳播委員會，NCC重申簡訊實聯制僅供防疫目的使用，政府未曾違反承諾，報載法官吹哨者質疑相關資料於防疫目的外使用，實屬誤解，2021年6月20日，https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=3562&sn_f=46221（最後瀏覽日：2024年11月3日）。

33 李寧修，警察存取預防性資料之職權與個人資料保護：以監視器之運作模式為例，臺大法學論叢，48卷2期，頁429（2019年）。針對此一爭議，本文之具體建議請參考伍、三、（三）監督機制之相關說明。

# 肆、德國法之觀察

## 一、法制架構

### （一）COVID-19下之處理接觸資料之法令規範

德國於對抗COVID-19之過程中，亦遭遇到許多挑戰，期間聯邦政府就德國傳染病防治法（Infektionsschutzgesetz, IfSG）多次研擬修法草案[34]，期得有效因應最新之疫情變化，以下將以2022年3月18日修正後之版本為主，進行介析。

依據德國傳染病防治法第5條第1項第1句，聯邦議會（Bundestag）得依據德國傳染病防治法第5條第1項第6句所定標準，將疫情定位為全國規模之流行狀態（epidemische Lage von Nationaler Tragweite），一旦進入此狀態，聯邦健康部（Bundesministerium für Gesundheit）在不妨礙各邦職權之前提下，即得因應疫情發展，訂定命令或採行相應之防疫措施，包括醫藥管制、排除專利保護等[35]。一旦確認有傳染病病人、疑似傳染病病人、疑似傳播或帶原者，或有死亡者經認定確診、疑似確診或為帶原者，主管機關應即採行必要之防疫措施，特別是德國傳染病防治法第28a條及第29條至第31條中所定措施，但其仍應限於對防阻疫情傳播之必要範圍內為之。而為確保其屬有效且必要之手段，德國傳染病防治法第5條第9項亦要求聯邦健康部針對其所採行措施之規範效果，應委託獨立之專家進行外部評估，其應跨領域組成，並特別關注傳染病學及醫學觀點，研析前述措施之效果，該評估結果應

34 德國傳染病防治法制定於2000年7月20日，最近一次修訂為2022年3月18日。若以COVID-19疫情在歐洲開始蔓延之時間點（2020年2月）為基準，疫情爆發後，該法於2020年共進行6次修正，2021年共有10次修正，2022年至今（2022年3月）則有1次修正。所增修之內容大多與對抗COVID-19之防疫措施有高度關聯。

35 潘俊良，科技防疫與隱私保護之衡平——歐盟與德國之例，科技法律透析，32卷5期，頁21-22（2020年）。

於2022年6月30送交聯邦政府，而聯邦政府須於同年9月30日附具其意見，一併提交至聯邦議會。

為了對抗COVID-19，德國傳染病防治法第28a條第1項下所定屬於預防性之特別保護措施，包括：第1款（於公共空間維持社交距離之要求）、第2款（佩戴口罩之義務）、第2a款（出示已接種、已康復或檢驗證明之義務）、第4款（建立並推廣衛生觀念之義務）及第17款：「要求就顧客、賓客或參與活動者之接觸資料（Kontaktdaten）進行處理，以利於有感染COVID-19情形後，得以追溯並阻斷傳播鏈」，即是透過預先蒐集、儲存民眾之接觸史，以備疫情爆發時，進行足跡追溯及匡列接觸者之不時之需。但隨著變種病毒相繼問世，疫情不斷延燒，2021年11月22日修正公布之德國傳染病防治法第28a條第7項中，更進一步允許即便於非屬全國規模流行狀態下，仍得採行必要之保護措施以防阻COVID-19[36]。而於該次修正中，增訂之同條項第8款，即曾要求針對曾經行經同條第1項第4款至第8款及第10款至第16款所稱公司、營業處所、機構、大眾交通運輸、活動、旅遊或從事相關運動者，就其接觸資料進行處理，並得優先使用由Robert Koch研究中心所研發Corona-Warn-App之QR Code所登錄資訊[37]，追蹤並阻斷傳染源，大幅擴張接觸資料蒐集之範圍。然而，隨著疫情趨緩，該款已自2022年3月18日修正之德國傳染病防治法中刪除[38]，將透過接觸資料進行足跡追溯之手段，回復屬在全國規模流行狀態下，方得採行之防疫措施。

---

36 但針對此種不受限於全國規模流行狀態下即可採行之保護措施，以及據同法第32條授權所訂定之相關命令，德國傳染病防治法第28a條第10項亦明定其至遲須於2022年9月23日失效。

37 關於Robert Koch研究中心所研發的Corona-Warn-App，其最初功能與「臺灣社交距離App」相當類似，係以藍牙技術記錄用戶之接觸史，以利日後在確定其曾與確診者近距離接觸時，能即時通知，並陸續擴充功能，增加透過QR Code掃瞄，讓其用戶得於同一App中記錄接觸史，並於足跡與確診者重疊時發送通知，且強調該資料僅儲存於用戶自身之使用裝置中；同時，為配合強化之防疫措施，更進一步支援儲存數位檢驗報告與疫苗接種紀錄之功能。

38 德國傳染病防治法第28a條第10項針對已據此公布之法令或採行之措施，明定

由於接觸資料必須得直接或間接地識別特定自然人，因唯有具備此特性，方得確保其可用於足跡追溯，故無疑屬個人資料之一種[39]，而德國傳染病防治法第16條第1項規定，當有事實足認，可能發生具傳染性之疾病，或經確認有前述情況時，主管機關應即採行必要措施，而於採行該等措施時，主管機關得蒐集個人資料，但所獲取之個人資料僅得基於本法之目的處理之。該規定應得作為主管機關基於防疫目的，蒐集、處理及利用個人資料之一般性規定。而針對德國傳染病防治法第28a條第1項第17款所稱接觸資料，德國傳染病防治法第28a條第4項進一步就其處理予以規範：要求控管者（Verantwortliche）僅得蒐集關於個人及其停留之時間與地點之訊息，並以追蹤該接觸者所絕對必要者為限（第1句）。控管者應確保未經授權者無從知悉所蒐集資料（第2句）。除了將資料移交給依據邦法進行蒐集之主管單位（zuständige Stelle）外，禁止將資料為目的外利用，且必須在蒐集後4週刪除之（第3句）。第3句所稱主管單位有權要求提供蒐集之資料，但以執行第25條第1項之追蹤接觸所必要者為限（第4句）。第1句之控管者於此情形負有將其所蒐集之資料，傳遞給第3句所稱主管單位之義務（第5句）。第3句所稱主管單位就該傳遞之資料，不得再為交付或作為接觸追蹤目的外之再利用（第6句）。經傳遞至第3句所稱主管單位之資料，若其已非屬進行接觸追蹤所必要，則應由其即刻以不可回復之方式刪除（第7句）。

德國傳染病防治法第32條第1句授權各邦政府，針對依據同法第28條、第28a條、第29條至第31條所採行之措施，得訂定命令進一步

---

其僅得實施至2022年4月2日，並以其屬修正後之第28a條第7項第1句及第8項第1句所定必要保護措施為限。

39 德國對於個人資料保護之定義，自歐盟個人資料保護基本規則施行後，即從其第4條第1款之規定：「『個人資料』係指有關識別或可得識別自然人（下稱『當事人』）之任何資訊；可得識別自然人係指得以直接或間接地識別該自然人，特別是參考諸如姓名、身分證統一編號、位置資料、網路識別碼或一個或多個該自然人之身體、生理、基因、心理、經濟、文化或社會認同等具體因素之識別工具。」

規定作為及禁止事項，以對抗傳染病。另外，聯邦政府依據德國傳染病防治法第28c條授權訂定之「COVID-19防護措施之例外命令」（COVID-19-Schutzmaßnahmen-Ausnahmenverordnung, SchAusnahmV）第7條中，亦授權各邦政府對於已接種疫苗（geimpft）、已康復（genesen）或已接受測試（getestet）者等3G族群，就其依據德國傳染病防治法所訂定之作為或禁止事項，得同中求異，各自訂定規範，採行緩解措施或列明例外情況。以巴伐利亞（Bayern）邦為例，由巴伐利亞邦健康照護部（Bayerische Staatsministerium für Gesundheit und Pflege, StMGP）所訂定之巴伐利亞傳染病防治措施規則（Bayerische Infektionsschutzmaßnahmenverordnung, BayIfSMV）[40]，亦曾透過處理接觸資料，力求阻絕疫情蔓延：包括1,000人以上於建築內、密閉空間、體育場館、其他出入受管制之場所中所舉行之任何形式聚會活動之舉辦者；以共同住宿形式經營之旅宿業者；酒吧、舞廳、聲色場所等類此娛樂場所之經營者；或是機關、法院及其他履行公共任務或執行公權力之公部門單位，均應／得藉由記錄進入上述場域者之姓名、地址、聯繫資訊（例如：電話或E-mail）及停留時間等接觸資料，以利未來足跡之確認與追溯。負有交付接觸資料義務者，應確保資料之真實性。接觸資料之蒐集亦得以電子之形式為之[41]。但隨著疫情趨緩及防疫策略之調整，透過預防性處理接觸資料以防阻疫情之作法，已自2022年2月16日公布、同年月17日生效之巴伐利亞傳染病防治措施規則中刪除，然而，其仍屬各

40 巴伐利亞傳染病防治措施規則係訂定於2020年3月27日，其自疫情爆發至今，亦經歷頻繁增修，現行法為2022年3月18日修正，同年月19日施行之第15版巴伐利亞傳染病防治措施規則（Fünfzehnte Bayerische Infektionsschutzmaßnahmen-verordnung, 15. BayIfSMV），施行期間也從原先規劃之4週，隨著修法一再延長，預計施行至2022年4月2日（巴伐利亞傳染病防治措施規則第12條）。

41 針對負有蒐集義務者，出於故意或過失而未蒐集接觸資料，或是負有義務提供接觸資料者，出於故意或過失提供錯誤之接觸資料，巴伐利亞傳染病防治措施規則皆將其列屬秩序違反（ordnungswidrig）之行為，並得依據德國傳染病防治法第73條第1a項第24款及同條第2項，處以2萬5千歐元以下罰鍰，但該罰則已隨著不再以處理接觸資料作為防疫措施而刪除。

邦於防疫時，依據德國傳染病防治法第28a條得選擇之防疫措施選項之一，未來是否可能「捲土重來」，值得持續關注。

### （二）歐盟個人資料保護基本規則之同步關注

由前述就德國規範架構之說明可知，其並未就採行之形式予以限制，然而，隨著疫情升溫，紙本表格之高成本和實用效益之低落，均促成德國積極嘗試運用科技輔助防疫，取代傳統書面紀錄，改以數位之形式，建置App行之，以求更有效地建立足跡追溯之系統。然而，既有之規範是否足以提供充分之法制基礎？就此，由德國聯邦及各邦個人資料保護監督機關共同組成召開之會議（Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, DSK），即一再發表聲明指出，現行法規在個人資料保護之層面仍有所不足，而亟待改善[42]，並指出於接觸資料之處理[43]過程中，應同步關注歐盟個人資料保護基本規則之相關規定[44]：

#### 1. 確認控管者及其所應擔負之責任

依據歐盟個人資料保護基本規則第4條第7款，所謂「控管者」

42 Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2021), Kontaktnachverfolgung in Zeiten der Corona-Pandemie – Praxistaugliche Lösungen mit einem hohen Schutz personenbezogener Daten verbinden, Datenschutzkonferenz, online verfügbar unter https://www.datenschutzzentrum.de/uploads/dsk/20210326_DSK-Stellungnahme_Kontaktnachverfolgung.pdf, S. 1.

43 歐盟個人資料保護規則所稱「處理」，「係指對個人資料或個人資料檔案執行任何操作或系列操作，不問是否透過自動化方式，例如蒐集、記錄、組織、結構化、儲存、改編或變更、檢索、查閱、使用、藉由傳輸加以公開、傳播或以其他方式使之得以調整或組合、限制、刪除或銷毀（歐盟個人資料保護規則第4條第2款）」，其實已將個人資料保護法中所稱「蒐集」、「處理」及「利用」之概念，均包含在其中。

44 Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2021), Einsatz von digitalen Diensten zur Kontaktnachverfolgung anlässlich von Veranstaltungs-, Einrichtungs-, Restaurants- und Geschäftsbesuchen zur Verhinderung der Verbreitung von Covid-19, Datenschutzkonferenz, online verfügbar unter https://www.datenschutzkonferenz-online.de/media/oh/20210429_DSK_OH_Kontaktnachverfolgung.pdf, S. 2-11.

係指單獨或與他人共同決定個人資料處理之目的與方法之自然人或法人、公務機關、局處或其他機構；若涉及兩個或兩個以上之控管者共同決定處理之目的及方式時，其即屬歐盟個人資料保護基本規則第26條所稱之「共同控管者」。共同控管者應以透明之方式，彼此間安排，確定其各自履行義務之責任（歐盟個人資料保護基本規則第26條第1項）。故，運用App之過程中，其中所涉及之系統業者、主管機關以及場所業者，應屬共同控管者，其等應以書面明確劃分其責任歸屬，包括：告知義務之履行、採行風險評估之責任、當事人主張權利時之應處等，且就當事人權利之主張，應對任一控管者皆得為之（歐盟個人資料保護基本規則第26條第3項）。

2. 釐清處理之合法性

針對運用App之過程中，涉及之共同控管者，亦應分別探究其處理個人資料行為之合法基礎：首先，App業者基於履行與其註冊用戶間契約所必要，而處理用戶之一般個人資料（歐盟個人資料保護基本規則第6條第1項第b款）；若涉及歐盟個人資料保護基本規則第9條第1項所稱特種個人資料時，則應依據歐盟個人資料保護基本規則第9條第2項第a款，取得當事人之明確同意。其次，就場所業者而言，於德國傳染病防治法第28a條第1項第17款以及各邦就COVID-19各自訂定之規則中，均得見要求其蒐集與應主管機關要求傳遞接觸資料之相關規定，且其亦合於歐盟個人資料保護基本規則第6條第1項第c款[45]及第9條第2項第i款[46]，針對一般個人資料及特種個人資料所定處理合法要件。最後，主管機關作為控管者，其

45 歐盟個人資料保護基本規則第6條第1項第c款：「合法之處理應至少符合下列要件之一：……（c）處理係控管者為遵守法律義務所必須者」。

46 歐盟個人資料保護基本規則第9條第2項第i款：「有下列情形之一者，不適用第1項規定：……（i）處理係基於公共衛生領域之公共利益，例如為防止對於健康之跨境嚴重威脅或為確保醫療保健及醫療產品或醫療設備品質之高標準與安全性而有必要者，並依據歐盟法或會員國法律規定採取適當及具體安全措施保護當事人之權利和自由，尤其是職業秘密」。

除依據德國傳染病防治法第28a條第4項第4句處理接觸資料外，歐盟個人資料保護基本規則第6條第1項第e款、第3項第b款（一般個人資料）[47]以及第9條第2項第i款（特種個人資料），均可能作為其合法處理之依據。

3. 基本原則之遵循：目的拘束原則、完整性與秘密性以及最少蒐集原則

依據歐盟個人資料保護基本規則第5條第1項第b款所定目的拘束原則，要求蒐集目的須特定、明確及合法，且原則上不得為該等目的以外之處理。德國傳染病防治法第28a條第4項實已明文禁止接觸資料為目的外利用（第3句），亦不許主管機關再為傳遞或作為追蹤目的以外之利用（第6句）。DSK指出，為遵循德國傳染病防治法所揭示嚴格目的拘束之意旨，若屬為提供未來作為其他目的處理所採行之去識別化措施，亦應一併禁止。另外，應採行適當安全之方式處理，確保資料之完整性與秘密性（Integrität und Vertraulichkeit），包括透過技術或組織上措施之採行，防免個人資料之未經授權或非法處理，並防止意外遺失、破壞或損害（歐盟個人資料保護基本規則第5條第1項第f款）。最後，則應將資料之處理限於適當、相關且處理目的所必要之範圍內，以落實資料最少蒐集原則（歐盟個人資料保護基本規則第5條第1項第c款）。

4. 保障當事人之權利

DSK強調，接觸資料之蒐集不必然一定以數位形式為限，為避免造成歧視並促進最大參與，應給予當事人有自由選擇提供接觸資料形式之機會。惟於向當事人蒐集資訊前，應以易見、易懂且清晰

47 歐盟個人資料保護基本規則第6條第1項第e款：「合法之處理應至少符合下列要件之一：……（e）處理係為符合公共利益執行職務或委託控管者行使公權力所必須者」；第3項第b款：「第1項第c款及第e款所定處理之依據應為：……（b）控管者受拘束之會員國法律」。

易讀之方式，告知歐盟個人資料保護基本規則第13條或第14條所定資訊，包括控管者及受託者身分之揭露、處理目的及依據之說明、當事人所得主張之權利以及向何人提出等。

當事人作為資料主體，自應尊重其權利之行使，例如：當事人得要求控管者確認，其是否處理以及處理何種個人資料，並得請求交付該資料之副本（歐盟個人資料保護基本規則第15條）；當事人應有權使控管者更正其不正確之接觸資料（歐盟個人資料保護基本規則第16條），並於追溯足跡之目的達成或保存期限屆至後，得要求控管者刪除之（歐盟個人資料保護基本規則第17條）。

5. 採行技術上及組織上適當措施

依據歐盟個人資料保護基本規則第32條第1項，考量現有技術，執行成本，處理之性質、範圍、脈絡、目的以及對當事人權利及自由所致風險發生之可能性及嚴重性，控管者及受託者應採行技術上及組織上適當措施，以確保風險立於適當可控之範疇[48]。此一資料安全維護措施，應由控管者於處理資料前，妥善規劃適當之科技化且有組織的措施，如：假名化（Pseudonymisierung）[49]，且該等措施應得確保資料保護原則之實踐，如資料最少蒐集原則，並採取有效方法且將必要保護措施納入處理程序，以符合歐盟個人資料保護基本規則之要求並保護當事人之權利（歐盟個人資料保護基本規則第25條）。

48 關於技術及組織上適當措施之建議，DSK另外發布有「標準－資料保護模型」（Standard-Datenschutzmodell），請參考 Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2019), Das Standard-Datenschutzmodell, Standard-Datenschutzmodell, online verfügbar unter https://www.datenschutzkonferenz-online.de/media/ah/20191106_SDM-Methode_V2.0.pdf.

49 歐盟個人資料保護基本規則所稱假名化，「係指處理個人資料之方式，使該個人資料在不使用額外資訊時，不再能夠識別出特定之資料主體，且該額外資料已被分開存放，並以技術及組織措施確保該個人資料無法或無可識別出當事人。」（歐盟個人資料保護基本規則第4條第5款）。

DSK藉此指出進行接觸足跡追蹤時，在個人資料保護法制部分，應相應關注之面向，亦以個人資料保護監督機關之身分，在疫情快速發展，法規變動顯得力有未逮之時，提出過渡期間之因應之道。

## 二、運作模式

### （一）紙本表格

關於接觸資料之蒐集，由於各邦均經授權得採行不同之作法，但其仍皆以德國傳染病防治法第28a條第1項第17款及同條第4項之規定為共同之基礎框架，以巴伐利亞傳染病防治措施規則（BayIfSMV）於2022年2月17日前曾就處理接觸資料所為規範為例，接觸資料中應記錄之資訊，包括：姓以及名、聯繫資訊（電話、E-Mail或住址得擇一）及停留日期與時間，每一家戶可由一人登記實聯制即可，所登載資料應確保其真實性。紙本上應登載其蒐集之法規依據，以及依據歐盟個人資料保護基本規則第13條第1項及第2項所要求於直接向當事人蒐集個人資料時所應告知之事項，包括：

－負責處理所蒐集個人資料之控管者：名稱，負責人，地址。
－資料保護監察機關之聯絡資料：地址，Email。
－資料處理之目的及合法基礎：作為確診COVID-19之情形進行接觸者之調查。依據歐盟個人資料保護基本規則第6條第1項第c款連結巴伐利亞傳染病防治措施規則第6條[50]以及德國傳染病防治法第28a條第4項。
－接觸資料之接收者（Empfänger）：若屬於確診COVID-19之情形進行接觸者調查所必要，應該要應健康主管機關之請求，傳遞蒐集資料。主管機關不得將該資料作為其他目的利用。參考德國傳染病防治法第28a條第4項第3句。

50 該條文已於2022年2月16日修正時刪除。

－保存期間：接觸資料將被保存4週後銷毀（德國傳染病防治法第28a條第4項第3句）。

－您對於該資料處理所得主張之權利：您作為所蒐集個人資料之當事人，得主張查詢權、更正權以及刪除權，您得向控管者行使權利。您有權向個人資料保護監察機關提出申訴（巴伐利亞資料保護監察局（Bayerisches Landesamt für Datenschutzaufsicht, BayLDA），地址，電話，官方網站申訴頁面之網址及連結）。

### （二）數位形式：以Luca App為例

Luca係由設於德國柏林之culture4life有限責任公司於2021年所開發建置的數位足跡追蹤系統[51]，其適用範圍限於德國境內，預期透過此App之使用，改善以紙本方式紀錄民眾接觸史的高成本及不便利性，並減輕場所業者之記錄義務，Luca一推出，即備受各界關注，德國多個邦及地方之衛生單位，皆已宣布採用該系統進行足跡追蹤[52]，其使用之場域包含各類場所，從酒吧、餐廳到各式活動，例如宗教或政治聚會，婚禮或生日派對，亦有置入學校或其他教育機構之討論。

Luca之用戶並不限於自然人，不論是個人、機關或營業場所，欲使用Luca登錄或記錄接觸資料，須先提供真實姓名／名稱、聯絡方式（手機，並選填E-Mail）與地址，經過身分認證成功後註冊成為用戶，取得專屬QR Code。當進出須紀錄接觸資料之場合時，可選擇提供自身專屬QR Code供掃瞄，或亦可選擇掃瞄該場所之專屬

51 關於Luca App，請參考https://www.luca-App.de/（最後瀏覽日：2024年11月3日）。

52 Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2021), Stellungnahme zu Kontaktnachverfolgungssystemen – insbesondere zu „Luca“ der culture4life GMBH, Datenschutzkonferenz, online verfügbar unter https://www.datenschutz.bremen.de/sixcms/media.php/13/DSK-Stellungnahme_LUCA_29-04-2021.pdf, S. 1; Der CCC: Quasi-Zwang zur Luca-App, ZD-Aktuell, 05295 (2021), S. 1.

QR Code，完成所謂「check-in」之登錄程序，但因Luca之運作須依賴網際網路，故用戶須確保其登錄時網路之暢通[53]。透過「check-in」之登錄程序，將建立一包括加密之用戶資料，造訪日期、時間以及加密場所資訊之檔案，儲存於用戶之裝置與Luca之後端伺服器中。當發現有確診者時，主管機關得要求Luca提供確診者過去14天之接觸資料，進行足跡追溯，並得進而確認與確診者足跡重疊者之紀錄；一旦確認Luca用戶曾與確診者在同期間共處於同一地點或場所，主管機關亦會透過App對用戶進行示警；Luca用戶得隨時於App中下載其過去28天之接觸資料進行查閱，並會定期收到不同程度示警之通知，例如：「可能之感染風險：您曾經停留在風險區域」、「提高之感染風險：主管機關調閱了您的資料」、「可能感染之群聚：於此場合出現疑似感染之情形」等[54]。

DSK對於導入Luca紀錄足跡，原則上持相當正向之見解，其認為數位形式輔以適當之技術，不論是透過加密確保資料之安全、得以設定於一定期間自動刪除資料、業者無須蒐集民眾具識別性之個人資料，皆是較紙本更佳的選擇[55]。但DSK對於Luca採行集中式資料庫之儲存方式，且主管機關所須之解鎖金鑰，若均係由Luca後端伺服器管理之情況下，認為將提高使用之風險，針對系統之安全性應以更高之標準檢證，因此，對於Luca願意公開其原始碼，以利公眾瞭解其運作機制，並藉由第三方測試，不斷修正其功能與設定，並採行資料保護影響評估（Datenschutz-Folgenabschätzung），認同

53 但用戶亦可選擇將專屬QR Code印出，隨身攜帶提供掃瞄，作為未使用智慧型手機或網路不穩定情形下的替代方案。

54 關於Luca App之運作方式及使用技術，*See* Theresa Stadler, Wouter Lueks, Katharina Kohls & Carmela Troncoso, *Preliminary Analysis of Potential Harms in the Luca Tracing System*, CORNELL UNIVERSITY (Mar. 22, 2021), https://arxiv.org/abs/2103.11958.

55 *Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder* (Fn. 42), S. 1.

其努力，但DSK仍建議儲存方式應儘可能避免集中[56]，並強調當事人以及業者仍應享有自由選擇留存資料方式之可能性[57]，且如同紙本蒐集所得接觸資料，以數位形式蒐集之資料亦禁止為目的外利用，不論是防疫以外之追蹤／定位服務、系統改善、預測功能等，均應禁止。

## 三、初步觀察

德國在接觸資訊之處理，主要係透過德國傳染病防治法及依其授權訂定之聯邦及各邦命令，建構其法制框架，所以自2020年2月間，COVID-19疫情開始在歐洲攻城掠地後，德國聯邦及各邦之相關法規亦頻繁地增修，以為因應。相較於臺灣，德國之立法機關及行政機關，似較傾向在常態之法制框架下，對抗非常態之COVID-19。但德國針對數位形式之蒐集，仍是既期待又怕受傷害，期待因數位形式帶來的便捷，甚至能夠提高對抗疫情之戰鬥力，然而不可諱言，針對如何運用個人資料於防疫，在尚未有健全之法規作為後盾之情況下，德國面對使用Luca記錄人民接觸資料，可能面臨的個人資料保護議題，目前皆是由德國之聯邦及各邦之個人資料保護專責機關共同研商，並積極透過提供意見（Stellungnahme）、指導（Orientierungshilfe）、決議（Entschließung）等方式，協助業者與地方衛生主管機關釐清個人資料保護法上可能衍生之爭議，但DSK亦呼籲，正本清源之道仍應制定全國一致之規範，以資遵循。由於我國目前仍欠缺專責、獨立個人資料保護主管機關，相較於德國個人資料保護專責機關積極就涉及個人資料保護爭議問題之主動表態，對於人民個人資料之保護所得發揮之影響力，確實較顯薄弱。

---

56 *Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder* (Fn. 42), S. 2.

57 *Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder* (Fn. 52), S. 3.

自2022年2月中旬起，德國各邦針對接觸資料處理之相關規範，雖大多皆已修法將其刪除，使其「暫時」自防疫措施中退場，但觀察過去德國對於接觸資訊之蒐集，不論是紙本或數位之形式，實際上皆要求填具真實之姓與名，錯誤填報甚至將面臨金額不低之罰鍰，與我國之實聯制有間。而針對Luca，其安全維護措施受到高度關注，就其將蒐集所得之接觸資料，以偏向集中式之資料儲存方式管理，因而相對提高了資料被竊取、洩漏或竄改之可能性，DSK亦表達了憂慮，其雖已採行資料保護影響風險評估，亦公開原始碼供各界檢驗，但資料庫之運作仍必須持續監督管理，以確保安全無虞。

## 伍、代結語：對於實聯制應具備法制框架之思考

### 一、回歸常軌：法律保留層級之檢視

在COVID-19大流行前，實聯制並未被廣泛運用於過往之傳染病防治中，故僅得被歸類為傳染病防治法第37條第1項第6款之「其他經各級政府機關公告之防疫措施」，至今並未就實聯制之特性，於傳染病防治法中制定專屬之要件及程序，而係由衛福部訂定實聯制指引，供各界遵循；反觀德國，其亦係於此次面臨COVID-19，方於2020年11月，增訂德國傳染病防治法第28a條，將接觸資料之蒐集、處理及利用納入規範，各邦亦基於授權，訂定各邦之規定，而為因應疫情之變化與管制手段之調整，前述規範均經過多次修正，甚至從2022年2月中起，透過修法逐步限縮其採行之範圍或不再以接觸資料之蒐集、處理及利用作為現階段之防疫手段。

我國於2021年5月26日起擴大實聯制之實施，簡訊實聯制亦同步應運而生，主要係因應升級為COVID-19第三級疫情警戒，應屬緊急事態下所採行之手段，然而，隨著疫情漸趨穩定，甚至是逐漸

轉變為與病毒共存之常態時，繼續採行實聯制之必要性，亦應配合進行滾動式檢討，包括就該手段與目的間之正當合理關聯，及其是否屬達成目的所必要，主管機關應負舉證說明之義務，若仍欲持續延用，其法制架構確實有升級之需求。由於實聯制屬預防性蒐集人民之個人資料，即使防疫屬重要公益目的，然考量此種近乎強制且大規模地蒐集人民足跡資料之行為，仍將對資訊隱私權帶來相當程度之干預，在法律保留層級之擇定，建議應以法律或依據法律具體明確授權訂定之法規命令為宜。

惟基於防疫目的蒐集、處理及利用個人資料之行為，相當多元，實聯制僅是其中一種型態，故針對此次對抗COVID-19疫情之過程中，曾運用個人資料防疫之措施，應一併盤點，若確實有助防疫，則應可參酌德國傳染病防治法之立法體例，將其自概括之「**其他經各級政府機關公告之防疫措施**」升格，明確例示，關注其與一般蒐集、處理及利用個人資料行為之不同，關注防疫過程中重預防、貴迅速之特性，將其合法要件，包括程序與組織之相應配套，予以明定，特別是針對配合當代設備、技術發展，相應而生之科技防疫措施，更應特別關注其對資訊隱私權可能帶來的新型態風險，對於國家之預防性資料蒐集行為，建立符合時代發展及需求之法制框架。

## 二、當事人權利之尊重與維護

隨著科技的發展與進步，資料之蒐集與傳遞不再侷限於特定形式，在數位化的資料處理模式下，個人資料被儲存及利用之型態更為廣泛多元，國家於此應加倍關注「人民有權決定其個人資料之公開與運用」此一受大法官肯認之憲法價值，因此，當國家基於對其他法益的維護而須限制人民之資訊隱私權時，除應具備公益之考量外，亦須考量資料之性質，蒐集、處理及利用之規模，以法律明確規範其限制之要件、範圍與方式，使人民充分瞭解，更應注意謹守

比例原則[58]，且即使係在符合前述要求之前提下合法蒐集、處理及利用個人資料，仍應隨時關注當事人權利於此過程中之尊重與維護。

在尊重當事人自主控制權利的第一個觀察面向，在於實聯制之實施方式，仍宜留給當事人有自行選擇之空間，因此，應避免僅提供單一執行實聯制之方式，除了簡訊實聯制外，仍應允許人民有選擇紙本實聯制之可能性。其次，實聯制指引中所規定之告知事項，納入個人資料保護法第3條明定之當事人權利類型及其行使方式，應屬對當事人權利尊重之展現，值得贊同，然而，一旦當事人不同意提供個人資料，而致使其須承受不利益之結果，例如：無法參與特定活動或課程，而該影響已對其權益致生損害，則仍應許其依據事件之性質，提請相應之救濟。最後，針對簡訊實聯制使用情形，目前衛福部疾管署建置有「民眾資料調閱紀錄查詢服務」，提供人民自行至網站進行查詢，或許值得進一步思考者為，將其轉換為由主管機關主動告知之可能性，參考通訊保障及監察法第15條就通訊監察明定結束後應即通知被監察人之規定，當人民之實聯制簡訊經地方主管機關調取，則於疫調結束後，地方主管機關應即主動通知當事人（不論其有無被匡列或是否須採行進一步之防疫措施），並簡要告知調取之原因及調查之結果，使其得藉此掌握其個人資料之使用歷程，尊重當事人就其個人資料之自主控制權利[59]。

## 三、組織與程序之要求

### （一）告知義務

憲法保障每個人對於自身之個人資料享有自主控制之權利，因

58 *Christian Bumke/Andreas Voßkuhle*, Casebook Verfassungsrecht, 7. Aufl., 2015, S. 99-100; *Helge Sodan* (Hrsg.), Grundgesetz: Beck'scher Kompakt-Kommentar, 2009, S. 40.

59 關於課予利用機關紀錄與告知義務之說明，請參考李寧修（註33），頁425。

此在個人資料保護法制中往往得見當事人同意與蒐集機關告知義務之相關規定，藉此確保個人資料之當事人對於其個人資料之蒐集、處理及利用之知情並進一步選擇的權利。一旦缺乏告知義務之規制，人民之個人資料雖由國家依法蒐集，但何時會被利用？如何利用、基於何種目的之利用？當事人皆無法掌握，恐導致人民生活在隨時被監控之恐懼之中，亦等同被剝奪其作為個人資料主體所得主張之任何權利[60]。

實聯制指引第2點所定告知事項，應屬允當，但告知之內容是否確實揭示與傳達，實聯制指引中允許「多層次告知」之方式，與歐盟個人資料保護基本規則區分必要告知事項（歐盟個人資料保護基本規則第13條第1項、歐盟個人資料保護基本規則第14條第1項），輔以進階告知事項（歐盟個人資料保護基本規則第13條第2項、歐盟個人資料保護基本規則第14條第2項）之方式，不謀而合，提供蒐集者彈性呈現告知內容之空間，亦可避免資訊過多而導致閱讀倦怠之情形。惟告知應如何以精準、透明、易懂且方便取得之格式，並考量當事人各別之情形，使用清楚且簡易之語言，確實傳達告知事項，或許可發揮創意，善用科技輔助，以更多元之形式，例如：語音廣播、影片、圖卡等，達到資訊傳遞之效果。另外，在告知事項部分，如同前述關於當事人權利維護之說明，告知內容亦應善盡相關救濟途徑之揭示，讓當事人有表達不服之機會，參考歐盟個人資料保護基本規則第13條第2項第d款及第14條第2項第e款所規定之進階告知事項中，即包括「向監管機關提起申訴之權利」之告知，此應屬對於當事人權利保障中應有之基本配備。

### （二）事前之資料保護影響評估

我國個人資料保護法較傾向透過事中之安全維護、事後處罰與損害賠償，作為管控之重點，個人資料之事前風險結果評估，尚未

60 李寧修（註33），頁424。

納入蒐集、處理及利用個人資料之要件，或是作為安全維護措施之必須選項。所謂的風險評估，應是立基於一般人民對於科學根據的信賴，以獨立、客觀、透明的方式對風險進行評價。透過風險評估，以科學之觀點衡量危害或是風險的規模及強度，預先發現可能對當事人之權利產生風險的因素，提供是否須先採行抑制或保護措施之決策參考。隨著大數據時代的來臨，資料蒐集之規模逐漸擴張，運用個人資料之形式益發日新月異，其影響層面亦趨廣泛，於事前採行個人資料保護影響評估確有其必要性[61]。

歐盟個人資料保護基本規則第35條明定資料保護影響評估，凡特定類型的個人資料處理，特別是使用新科技，並考量其性質、範圍、情境及目的，可能對自然人的自由及權利產生高度風險時，控管者應先針對預計資料活動對個人資料保護的影響，進行評估（歐盟個人資料保護基本規則第35條第1項）。而應採行影響評估之具體情況，包括：

－基於個人資料的自動化處理，包括剖析，對自然人個人進行系統性及大規模的分析，並據以對特定個人作成具有法律效果的決定或產生類似影響；
－大規模蒐集、處理或利用第9條第1項規定的特種個人資料或第10條規定的前科資料；
－大規模且系統性地監控公眾場所。

依據歐盟個人資料保護基本規則第35條第7項，資料保護影響評估至少應涵蓋之面向，包括：

－對於預計進行的蒐集、處理或利用活動及其目的的系統性描述，包括：資料管理者所主張的合法利益；
－蒐集、處理或利用活動達成目的必要性與比例性的評估；

61 李寧修（註17），頁41。

－對於資料當事人自由與權利所造成風險的評估；
－回應風險所預計採取的措施，包括保護措施、安全措施，以及考量資料當事人與其他關係人權利與合法利益，確保個人資料保護與符合本規則要求所採取的機制。

實聯制指引第4點規定，機關以資訊系統或App實施實聯制者，應進行資訊安全風險評估，採行相符安全控制措施，確保系統安全防護水準。該「資訊安全風險評估」，應屬形塑適當安全維護措施之內涵時，得進一步思考之方向。考量實聯制之形式眾多，該資訊安全風險評估之範圍，建議可參考前述歐盟個人資料保護基本規則之規定，由個人資料保護之主管機關提供具體之規範及作法，例如：透過公告必須採行風險評估之「黑名單」或無須採行風險評估之「白名單」（歐盟個人資料保護基本規則第35條第4項及第5項），將實施範圍限於運用資訊系統蒐集實聯制資料之公務及非公務機關；而針對使用相同性質或技術之系統，應得進行共同之風險評估，以適度降低風險評估之成本等[62]。

### （三）監督機制

實聯制中所蒐集之資料，是否誠如實聯制指引所稱「禁止目的外利用」、「僅留存28天」、「屆期主動刪除或銷毀」，若得有相應之監督機制，應屬重要且必要。首先，由權力分立之角度觀察，主管機關對於採行實聯制之情形及效果，應負有向國會及公眾報告之義務，並公開相關資訊，提高其透明性，接受民意之檢視與監督，於嚴重特殊傳染性肺炎防治及紓困振興特別條例第18條（已於2023年7月1日廢止）中，課予行政院就疫情與預算執行向立法院報告之義務，應得收權力監督、制衡之效。

62 關於引進資料保護影響評估之具體建議，請參考張陳弘（註18），頁358-366；劉定基，臺灣政府資料開放的現況與難題——以個人資料保護為觀察中心，收於：台灣行政法學會編，行政執行／行政罰／行政程序／政府資料開放／風險社會與行政訴訟，頁314-316（2017年）。

其次，實聯制指引第3點要求蒐集機關，不論是公務機關或非公務機關，應「採行適當之技術上及組織上安全措施，並指定專人辦理安全維護事項」。觀諸德國在個人資料保護法制之監管機制設計中，亦藉由課予資料控管者及受託處理者設置個人資料保護長（Datenschutzbeauftragte）之義務，達到監管之目的：其一，針對公務單位，包括參與市場競爭之公營事業，德國聯邦個人資料保護法（Bundesdatenschutzgesetz）第5條要求應設置個人資料保護長，但可視其組織型態與規模，由多個公務單位任命共同之個人資料保護長。德國聯邦個人資料保護法第7條特別強調其所擔負之任務，至少包括：

－針對負責處理個人資料之公務單位及其所屬人員，告知其依據本法或其他與個人資料保護相關法令，包括為轉化歐盟第2016/680號指令所發布之法令，所負有之義務並提供諮詢；
－監管本法或其他與個人資料保護相關法令之遵行，包括為轉化歐盟第2016/680號指令所發布之法令，以及公務單位對於個人資料保護所採行之策略，包括對於資料受託處理者之職務分配、敏感化、教育訓練，和與其相關之審查；
－提供與個人資料保護影響評估相關之諮詢，並依據本法第67條監督其實施情形；
－與監督機關共同合作；
－就與處理個人資料相關之疑義，作為監督機關之對口單位，包括依據本法第69條所採行之事前協商以及針對其他問題所提供諮詢。

其二，對於非公務單位，德國聯邦個人資料保護法第38條明定，具有20人以上專責自動化處理個人資料規模之非公務單位，應設置一名個人資料保護長[63]。另外，針對依據歐盟個人資料保護基

63 2019年德國聯邦個人資料保護法修法時，將非公務單位處理個人資料之人數，

本規則第35條負有採行個資影響評估義務之控管者或受託者，或是其業務上基於（匿名）傳送個人資料之目的或進行市場或意見調查之目的而處理個人資料時，則不受前述受託者數量之限制，均應即任命個人資料保護長。

由上述可知，該「專人」若循德國個人資料保護長之模式設置，應得有效強化機關內部之自律管控，然而，觀諸其所擔負之任務，該「專人」應享有之資源及支持，實涉及制度層面之規劃與法令之配合，方有可能發揮預期之監督功能，恐非一蹴可幾。

最後，仍是應建置獨立、專責之個人資料保護監督機關。目前我國個人資料保護法雖仍係採分散式管理，但隨著憲法法庭111年憲判字第13號判決之作成，立法院業已通過個人資料保護法第1條之1[64]，新設個人資料保護委員會為個人資料保護之監督機關[65]，目的在於確保個人資料蒐集、處理及利用，均符合個人資料保護法規定，以完足對人民資訊隱私權之保障。但該條文目前仍待行政院定施行日期，待其正式施行後，個人資料保護委員會將作為個人資料保護法之主管機關，而其組織形式及後續於個人資料保護之監管作為，值得持續關注。

反觀德國個人資料保護監督權責之劃分，由於其係採行聯邦體制，於聯邦層次設有聯邦個人資料保護暨資訊自由監察官（Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,

---

由原先之10人提升為20人，適度放寬設置個人資料保護長之門檻，以減輕小型企業之負擔。

64 個人資料保護法第1條之1：「本法之主管機關為個人資料保護委員會（第1項）。自個人資料保護委員會成立之日起，本法所列屬中央目的事業主管機關、直轄市、縣（市）政府及第五十三條、第五十五條所列機關之權責事項，由該會管轄（第2項）。」

65 國家發展委員會，立法院三讀通過個資法修正案 將強化企業個資外洩罰責 並盡速設置個資保護委員會籌備處，2023年5月16日，https://www.ndc.gov.tw/nc_27_36901（最後瀏覽日：2024年11月3日）。

BfDI），作為最高聯邦機關之一；於邦之層級，則分別設有邦之個人資料保護監察官（Landesbeauftragte für den Datenschutz, LfD），各邦多於其個人資料保護法中，規範其設立、組織及職權[66]。德國就個人資料保護所建置之監督機關，或許有值得我國未來參考者[67]，包括：

－個人資料保護之監督機關應具備獨立性，應屬目前個人資料保護法制中具有高度共識者。考量個人資料之蒐集、處理及利用，因涉及多方利益之權衡，此職權應交由具有獨立性之機關執掌。此一對於監督機關獨立性之要求，曾由德國聯邦憲法法院及歐洲法院在多次判決中大聲疾呼：個人資料保護之監督乃確保資訊自決權所不可或缺之把關機制，對此基本權利之侵害僅有在一獨立個人資料保護監察機關存在之前提下方得被允許[68]。

－針對執掌個人資料保護之監督機關，並非僅有單一機關，而係依據國家體制，分別由聯邦及邦共同擔當，並透過定期性之會議，作為聯邦及各邦監督機關相互溝通、交流之平臺。但均要求其須為「專責機關」，亦即該機關之設立，應以專門負責個人資料保護之監管為主。此與我國未來擬由個人資料保護委員會統籌中央及地方個人資料保護之權責，作為單一監督機關之作法，有所不同。

---

66 *Jürgen Kühling/Christian Seidel/Anastasios Sivridis*, Datenschutzrecht, 3. Aufl., 2015, S. 231. 於部分邦之個人資料保護監察官，亦同時擔負促進資訊公開之任務。

67 李寧修、翁逸泓，「歐盟國家個人資料保護法制因應GDPR施行之調適——以德國與英國為例」委託研究計畫結案報告（GRB系統編號：PG10805-0109），行政院國家發展委員會108年度委託研究計畫，執行期間：2019年5月10日至2020年5月9日，頁124-125。

68 Vgl. *Julia Kruse*, Der öffentlich-rechtliche Beauftragte, 2007, S. 207 ff.; *Dieter Zöllner*, Der Datenschutzbeauftragte im Verfassungssystem: Grundsatzfragen der Datenschutzkontrolle, 1995, S. 21 ff., 167-170; *Hans H. Wohlgemuth/Jürgen Gerloff*, Datenschutzrecht, 3. Aufl., 2005, S. 143-145.

－不論是設於聯邦或邦層級之個人資料保護監察官，均係採行首長制而非合議制，觀察我國目前所採行之分散式監管機制，同時有首長制及合議制機關者，而未來擬設置之個人資料保護委員會，若係規劃為中央三級之合議制獨立機關，此與德國現行監督機關之體制，確有所不同。

# 參考文獻

## 1. 中文部分

Christian Starck著，李建良譯（2006），基本權利之保護義務，收於：法學、憲法法院審判權與基本權利，頁411-496，臺北：元照。[Starck, Christian (1994), Grundrechtliche Schutzpflichten, in: ders., Praxis der Verfassungsauslegung, Baden-Baden: Nomos, S. 46-84.]

甘佳加（2021），警察使用人臉辨識系統查證身分的合法性研究——以M-Police即時相片比對功能為中心，國立臺灣大學法律學研究所碩士論文。

西德聯邦憲法法院著，蕭文生譯（1990），關於「一九八三年人口普查法」之判決，收於：西德聯邦憲法法院裁判選輯（一），頁270-326，臺北：司法周刊雜誌社。

何念修（2019），個資保護「適當之安全措施」——以新加坡個資法之技術措施建議為比較對象，科技法律透析，31卷1期，頁55-61。

何建志（2020），COVID-19疫情期間防疫與隱私之平衡：相關法律議題分析與社會正義觀點，台灣法學雜誌，387期，頁23-32。

吳采模、高塚真希（2020），「嚴重特殊傳染性肺炎防治及紓困振興特別條例」之概要及其法律問題，萬國法律，231期，頁107-115。

李建良（2020），在瘟疫中思索自由，人文與社會科學簡訊，22卷1期，頁30-33。

李崇僖（2020），在瘟疫蔓延中檢視個資保護法制，台灣法學雜誌，387期，頁39-43。

李寧修（2015），預防性通信資料存取之憲法界限——以歐盟儲備

性資料存取指令（2006/24/EG）之發展為借鏡，興大法學，17期，頁87-140。

———（2019），警察存取預防性資料之職權與個人資料保護：以監視器之運作模式為例，臺大法學論叢，48卷2期，頁391-437。

———（2020），個人資料合理利用模式之探析：以健康資料之學術研究為例，臺大法學論叢，49卷1期，頁1-50。

李寧修、翁逸泓（2020）「歐盟國家個人資料保護法制因應GDPR施行之調適——以德國與英國為例」委託研究計畫結案報告（GRB系統編號：PG10805-0109），行政院國家發展委員會108年度委託研究計畫，臺北：行政院國家發展委員會。

李震山（2001），論國家機關蒐集資訊之合法性，收於：國立政治大學傳播學院研究暨發展中心、理律法律事務所編，傳播與法律系列研討會（七）論文彙編：監聽法vs.隱私權——全民公敵？，頁1-50，臺北：三民。

李震山、許義寶、李寧修、陳正根、李錫棟、蔡庭榕、蔡政杰（2024），入出國及移民法逐條釋義，2版，臺北：五南。

林其樺（2018），數位時代個人隱私界線怎麼畫？——從美國Carpenter v. United States案淺介行動電話定位資訊之隱私合理期待，科技法律透析，30卷11期，頁11-15。

林欣柔（2020），防疫？妨疫？疾病監測、接觸者追蹤與個人資訊隱私之平衡，台灣法學雜誌，387期，頁45-52。

郭戎晉（2012），論數位環境下個人資料保護法制之發展與難題——以「數位足跡」之評價為核心，科技法律透析，24卷4期，頁18-39。

陳玥汝（2020），我國紓困條例所涉隱私議題初探，科技法律透析，32卷5期，頁26-32。

張陳弘（2021），科技智慧防疫與個人資料保護：陌生但關鍵的資料保護影響評估程序，臺大法學論叢，50卷2期，頁337-400。

黃昭元（2005），無指紋則無身分證？：換發國民身分證與強制全

民捺指紋的憲法爭議分析，收於：國際刑法學會臺灣分會編，民主、人權、正義：蘇俊雄教授七秩華誕祝壽論文集，頁461-508，臺北：元照。

劉定基（2017），臺灣政府資料開放的現況與難題——以個人資料保護為觀察中心，收於：台灣行政法學會編，行政執行／行政罰／行政程序／政府資料開放／風險社會與行政訴訟，頁295-322，臺北：元照。

潘俊良（2020），科技防疫與隱私保護之衡平——歐盟與德國之例，科技法律透析，32卷5期，頁19-25。

蔡庭榕（2020），我國與英國警察運用指紋個人識別載具適法性之比較分析，執法新知論衡，16卷2期，頁31-62。

## 2. 外文部分

Bumke, Christian/Voßkuhle, Andreas (2015), Casebook Verfassungsrecht (2008), 7. Aufl., Tübingen: Mohr Siebeck.

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2021), Kontaktnachverfolgung in Zeiten der Corona-Pandemie – Praxistaugliche Lösungen mit einem hohen Schutz personenbezogener Daten verbinden, Datenschutzkonferenz, online verfügbar unter https://www.datenschutzzentrum.de/uploads/dsk/20210326_DSK-Stellungnahme_Kontaktnachverfolgung.pdf.

——— (2021), Einsatz von digitalen Diensten zur Kontaktnachverfolgung anlässlich von Veranstaltungs-, Einrichtungs-, Restaurants- und Geschäftsbesuchen zur Verhinderung der Verbreitung von Covid-19, Datenschutzkonferenz, online verfügbar unter https://www.datenschutzkonferenz-online.de/media/oh/20210429_DSK_OH_Kontaktnachverfolgung.pdf.

——— (2021), Stellungnahme zu Kontaktnachverfolgungssystemen – insbesondere zu „Luca“ der culture4life GMBH, Datenschutzkonferenz,

online verfügbar unter https://www.datenschutz.bremen.de/sixcms/media.php/13/DSK-Stellungnahme_LUCA_29-04-2021.pdf.

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2019), Das Standard- Datenschutzmodell, Standard-Datenschutzmodell, online verfügbar unter https://www.datenschutzkonferenz-online.de/media/ah/20191106_SDM-Methode_V2.0.pdf.

Kruse, Julia (2007), Der öffentlich-rechtliche Beauftragte, Berlin: Duncker & Humblot.

Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios (2015), Datenschutzrecht (2008), 3. Aufl., Heidelberg: C. F. Müller.

Sodan, Helge (Hrsg.) (2009), Grundgesetz: Beck'scher Kompakt-Kommentar, München: C. H. Beck.

Stadler, Theresa, Wouter Lueks, Katharina Kohls, and Carmela Troncoso (2021), Preliminary Analysis of Potential Harms in the Luca Tracing System, In *Cornell University*, https://arxiv.org/abs/2103.11958.

Wohlgemuth, Hans H./Gerloff, Jürgen (2005), Datenschutzrecht (1992), 3. Aufl., Köln: Luchterhand.

Zöllner, Dieter (1995), Der Datenschutzbeauftragte im Verfassungssystem: Grundsatzfragen der Datenschutzkontrolle, Berlin: Duncker & Humblot.

# Preventative Process of Personal Information Based on the Purpose of Protection against Epidemic:

## Taking the Operation of Conduct Name Registration as an Example

*Ning-Hsiu Lee**

**Abstract**

At the end of the year 2019, the epidemic of severe pneumonia with novel pathogens (hereinafter referred to as COVID-19) breaks out from one country to another and overspreads fast to the whole world. In all cases, every country attempts to prevent the spread of the epidemic and tries to adopt different means and measures to fight this public health emergency. Among these means and measures, the governments commence on analyzing and applying the personal information to prevent and cure the COVID-19 by collecting, processing, and using personal information, and these have already been seen from time to time. This article aims at the operation of implementing the conduct name registration which is based on the purpose of preventing the epidemic. The conduct name registration is by collecting, processing, and utilizing people's personal information in advance to facilitate tracing back the footprint of every individual for identifying the source of the infection and avoiding the break out of the epidemic. Although it is well-intended, from the perspective of protecting the right to information privacy, the basic legal framework of the conduct of name registration should still be viewed carefully. This article will analyze the legal foundations, essentials, and the operation mode of the

* Professor, Department of Law, Chinese Culture University.

implementation of the conduct name registration, and induct the related controversies that may arise from collecting, processing, and utilizing the personal information. At the same time, not only compare with the operation mode of the conduct name registration but also its practices in German laws against the COVID-19 will also be observed as an example. At last, regarding the operation of the conduct name registration, this article will put forward personal observations and suggestions, in hope to provide some reference to the future development and reformation of the legal framework and practice of communicable disease control in Taiwan.

KEYWORDS: personal information, right to information privacy, COVID-19, conduct name registration, Communicable Disease Control Act, Personal Data Protection Act.