10915G0018

智慧建築安全監控資料應用之法制課題及對策之研究

受委託單位　：　財團法人資訊工業策進會
研究主持人　：　王自雄 主任
研究員　　：　周晨蕙

研究期程　　：　中華民國 109 年 1 月至 109 年 12 月
計畫經費　　：　新臺幣玖拾玖萬參仟貳佰元

內政部建築研究所委託研究報告

中華民國 109 年 12 月

（本報告內容及建議，純屬研究小組意見，不代表本機關意見）

目次

表次

圖次

摘要

關鍵詞：智慧建築、個人資料、資料應用

伴隨時代進步，物聯網、大數據、人工智慧等新技術開始應用於建築物，衍生許多創新應用服務。因應上述發展趨勢，行政院推動「數位國家·創新經濟發展方案（2017-2025）」及「前瞻基礎建設計畫」等重要政策，希望藉由數位產業帶動整體經濟發展，催生新興商業模式，內政部建築研究所「智慧化居住空間整合應用人工智慧科技發展推廣計畫」亦配合上述政策目標，積極推動新興科技於智慧化居住空間之應用。

智慧化居住空間之創新應用，例如智慧門禁系統、安全監控系統、健康照護，空調、照明、電梯等設備之節能管理等，可透過聯網設備或感測器蒐集個人生理及日常活動資料，以及設備使用狀況等數據，用於完善及提供相關服務。然而，由於個人生理資料或日常活動資料等，可能該當我國個人資料保護法上之個人資料，導致一般民眾對上述應用感到不安，加上歐盟一般資料保護規範（General Data Protection Regulation, GDPR）施行後，加強對歐盟境內個資蒐集和利用之保護，亦影響到其他與歐盟有交易往來之國家，使得智慧建築資料相關法律問題變得越來越複雜，成為業者推動相關應用研發之阻礙。

有鑑於此，為推動人工智慧等新技術應用於智慧化居住空間，達成利用數位產業帶動整體經濟發展之目標，本計畫擬以智慧建築之資料應用法制課題及對策為對象，並聚焦於智慧門禁系統及安全監控設備進行探討。本計畫首先將透過訪談業者，了解國內智慧門禁系統及安全監控設備之技術應用現況，然後針對應申請智慧建築標章之各類建築物，分析並歸納其蒐集、處理或利用個資之情境，對應我國個人資料保護法相關規定及司法實務，找出智慧建築安全監控資料應用可能存在之法制障礙。最後，本研究將根據上述現況調查及法制障礙分析結果，編寫問答集草案，希望能藉此協助業者落實個資法遵需求，建立可安心利用智慧建築資料之法制環境。

Abstract

keywords： smart building, personal data, data application

Smart building can gather information from the environment inside and outside to optimize temperature, lighting, and other elements. Because of this, Smart building can provide comprehensive, convenient, intelligent, and interactive services for both individuals and their surroundings. While Smart building bringing numerous benefits, it also causes severe threats to user privacy. The data that collected by Smart building, such as sensory data or contextual data, part of them could be seen as personal information. If someone want to design buildings or systems that collect and track any data with personal information, they must be compliant with regulation.

Not all company could bear the burden of regulation. For reducing the burden of regulation, this article research smart building data legal issue, and focus on security monitoring question. First of all, this article will interview related operator to understand actual situation, then analyze Personal Data Protection Act and judicial practice in Taiwan. At last, this article will according the above research, and draft FAQ of Smart building gathering personal information.

第一章 緒論

第一節 研究緣起

伴隨時代進步，物聯網、大數據、人工智慧等新技術開始應用於建築物，衍生許多創新應用服務。因應上述發展趨勢，行政院推動「數位國家·創新經濟發展方案（2017-2025）」及「前瞻基礎建設計畫」等重要政策，希望藉由數位產業帶動整體經濟發展，催生新興商業模式，內政部建築研究所「智慧化居住空間整合應用人工智慧科技發展推廣計畫」亦配合上述政策目標，積極推動新興科技於智慧化居住空間之應用。

智慧化居住空間之創新應用，例如智慧門禁系統、安全監控系統、健康照護，空調、照明、電梯等設備之節能管理等，可透過聯網設備或感測器蒐集個人生理及日常活動資料，以及設備使用狀況等數據，用於完善及提供相關服務。然而，由於個人生理資料或日常活動資料等，可能該當我國個人資料保護法上之個人資料，導致一般民眾對上述應用感到不安，加上歐盟一般資料保護規範（General Data Protection Regulation, GDPR）施行後，加強對歐盟境內個資蒐集和利用之保護，亦影響到其他與歐盟有交易往來之國家，使得智慧建築資料相關法律問題變得越來越複雜，成為業者推動相關應用研發之阻礙。

有鑑於此，為推動人工智慧等新技術應用於智慧化居住空間，達成利用數位產業帶動整體經濟發展之目標，本計畫擬以智慧建築之資料應用法制課題及對策為對象，並聚焦於智慧門禁系統及安全監控設備進行探討。本計畫首先將透過訪談業者，了解國內智慧門禁系統及安全監控設備之技術應用現況，然後針對應申請智慧建築標章之各類建築物，分析並歸納其蒐集、處理或利用個資之情境，對應我國個人資料保護法相關規定及司法實務，找出智慧建築安全監控資料應用可能存在之法制障礙。最後，本研究將根據上述現況調查及法制障礙分析結果，編寫問答集草案，希望能藉此協助業者落實個資法遵需求，建立可安心利用智慧建築資料之法制環境。

第二節 研究目的

智慧建築相關應用種類繁多，包括智慧門禁、自動車牌辨識、節能管理和健康照護等，其蒐集資料的主體、方式及蒐集的資料類型等均有所不同，本計畫僅針對智慧門禁系統及安全監控設備所蒐集之個人資料進行探討，合先敘明。

根據上述研究背景及範圍，本計畫之研究目的如下：

1. 透過調查國內外建築物門禁系統及安全監控設備之應用狀況，了解相關業者個資蒐集、處理及利用狀況，以及所遭遇的問題。
2. 盤點建築物門禁系統及安全監控設備之資料應用情境，對應我國個資法上相關規定及司法實務，分析可能影響上開應用發展之法制障礙。
3. 參酌國內外相關文獻，針對上述資料應用情境和法制障礙，完成編寫「推動智慧建築應用法制障礙及因應對策─安全監控篇」問答集草案，消弭民眾對於個資的不安，以及協助業界落實個資法遵要求，鼓勵業者投入相關應用研發。

第三節 研究方法與流程

一、研究方法

(一)深度訪談法

本研究將透過訪談業者，了解國內智慧門禁系統及安全監控設備之技術應用現況，以及業者蒐集或處理個資之方式和資料利用之範圍。

(二)文獻分析法

本研究將收集國內外有關智慧建築資料應用之法制問題及對策等文獻，整理我國學界和司法實務對於個資蒐集、處理及利用之意見，作為編寫問答集草案之參考。

二、研究流程

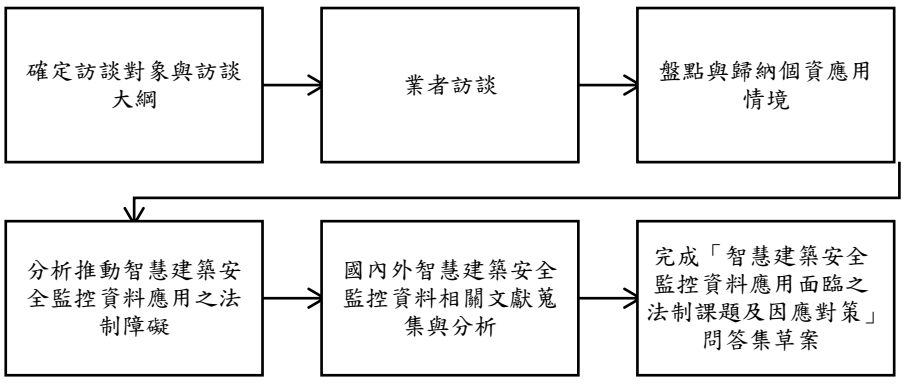


圖 1-1 研究流程圖

資料來源：本研究整理

第四節 預期成果與效益

根據上述研究目的，本計畫預期成果與效益如下：

1. 了解國內智慧建築門禁系統及安全監控設備於資料蒐集、處理及利用之現況，確認應優先處理及因應之問題。
2. 釐清我國個資法及相關規定對於智慧建築門禁系統及安全監控設備之限制，避免法令成為推動智慧建築創新應用之阻礙。
3. 協助資料蒐集主體於蒐集、處理、利用個人資料時落實個資法遵要求，排除可能觸法之疑慮，提高業者投入智慧建築市場之意願 。
4. 降低民眾對於智慧建築相關應用之牴觸，有利於進一步擴大智慧建築及相關智慧化應用市場。

第二章 智慧建築門禁及安全監控資料應用法制分析

第一節、 我國智慧建築定義與發展現況

(一) 我國法上之智慧建築定義與範圍

綜觀我國行政法規，於名稱或條文內提到智慧建築者只有《申請指定綠建築綠建材智慧建築標章評定專業機構收費標準》、《智慧建築標章規費收費標準》、《都市危險及老舊建築容積獎勵辦法》、《都市更新建築容積獎勵辦法》及《都市計畫法台灣省施行細則》。前兩者係與智慧建築標章收費有關之規定，後三者則係以智慧建築作為容積獎勵對象之規定，均未於法條中明文定義智慧建築，故想了解何謂智慧建築，僅能透過「智慧建築設計技術參考規範」或智慧建築標章等規範，一探智慧建築樣貌。

內政部於 2012 年訂定「智慧建築設計技術參考規範」，就各類型建築物智慧化之共通部份，依設置標準加以分級規範，並將建築物構成部份分為綜合佈線、資訊通信、系統整合、設施管理、安全防災、健康舒適、貼心便利與節能管理等指標，從設計觀點出發，整理歸納出建築物智慧化之設計規範，提供給智慧建築起造人、設計人、各專業技術及相關機關參考[1]。

除訂定設計技術參考規範外，內政部建築研究所自 2004 年起正式受理智慧建築標章之申請，以加速我國智慧建築發展，智慧建築標章評估項目歷經數次調整，根據 2016 年出版之智慧建築評估手冊中，可知智慧建築評估內容包括：綜合佈線指標、資訊通信指標、系統整合指標、設施管理指標、安全防災指標、節能管理指標、健康舒適指標和智慧創新指標等 8 項指標，每項指標之評估項目均分為基本規定和鼓勵項目 2 種，前者為智慧建築之門檻。在 2011 年出版之智慧建築解說與評估手冊中，八項指標與「智慧建築設計技術參考規範」相同，而在 2016 年出版智慧建築評估手冊時，為鼓勵智慧創新，將貼心便利指標改為智慧創新指標。儘管目前智慧建築標章評估項目和「智慧建築設計技術參考規範」略有差異，惟從上述 8 大指標之評估內容，仍可知曉我國行政機關想像中之智慧建築應具備之功能。

[1] 內政部營建署，《智慧建築設計技術參考規範》，頁 1（2012）。

表 2-1 智慧建築評估指標基本規定評估項目表

指標名稱	項目
綜合佈線	1.1 佈線規劃與設計、1.2 佈線應用與服務、1.3 佈線性能與整合、1.4 佈線管理與維運
資訊通信	2.1 廣域網路之接取、2.2 數位式（含 IP）電話交換、2.3 區域網路、2.4 公共廣播、2.5 公共天線
系統整合	3.1 系統整合基本要求、3.2 系統整合程度、3.3 整合安全機制
設施管理	4.1 資產管理、4.2 效能管理、4.3 組織管理、4.4 維運管理
安全防災	5.1 防火系統、5.2 防水系統、5.3 防盜系統、5.4 監視系統、5.5 門禁系統、5.6 停車管理、5.7 有害氣體防制、5.8 緊急求救系統
節能管理	6.1 能源監視、6.2 能源管理系統、6.3 設備效率、6.4 需量控制
健康舒適	7.1 室內高度

資料來源：智慧建築評估手冊（2016）

此外，根據內政部「智慧建築標章申請認可評定及使用作業要點」第 2 點，所謂智慧建築係指『藉由導入資通訊系統及設備之手法，使空間具備主動感知之智慧化功能，以達到安全健康、便利舒適、節能永續目的之建築物。』另根據內政部建築研究所公布之《智慧建築評估手冊》，其在序言指出『智慧建築是應用網路、監測設備及系統整合等技術，讓建築物達到自動感知、分析及回應等功能，並在規劃設計之初，事先考慮使用者需求，提供需要的服務及後續維護管理的方便性，使建築物在完成之後，可以有最佳化之組合與運轉，以滿足使用者對安全、舒適、便利、效率的需求，並達到節能與降低維護管理人力經費之目標。』亦可知智慧建築是應用資通訊技術，使建築物可滿足使用者需求之建築物。

上述有關智慧建築之評估項目或設計技術規範，或屬於獎勵性質之標章，或為不具強制力之行政指導，可知我國並未以法律規定何謂智慧建築。惟《建築技術規則》為配合智慧建築發展，除於第 116-1 條至第 116-7 條要求建築物之公共空間應設置各項安全維護措施，如照明裝置、監視攝影裝置、緊急求救裝置和警戒探測裝置，亦於建築設備篇第 8 章第 138-1 條規定設置中央監控室，可從上述規定一探我國法上智慧建築的樣貌。

(二) 智慧建築發展趨勢

建築物是近年智慧化重要應用之一，其中智慧家庭與智慧建築常被放在一起討論，但兩者的設計方向大不相同，前者主要訴求舒適與便利，而後者則著重節能與安全[2]。目前智慧建築有三大發展趨勢，分別是強調節能和創能之綠能環保；強調將感測器布建於建築物中，獲取各種資訊進行控管之智慧感

[2] 王明德，〈建構智慧建築系統延伸基本功能擴大市場〉，《SmartAuyo》，頁 56（2018）。

測，以及透過網路將所有資訊統一管理分析之萬物互聯[3]。

近年感測器之應用已經十分普遍，而建築內所用到的感測節點通常可分為安全、節能、便利與照護等用途，安全是針對個人與建築物之安全警示，如災害警示、緊急通報、有毒氣體偵測、門禁管理等；節能感測如電器、燈光與空調之能源偵測管理；照護感測如生理數據之偵測；便利感測如自行調整溫濕度、空氣品質等[4]。透過感測器之應用，我們可以廣泛蒐集更多建築物內資料進行分析，優化建築物內各項服務，提高生活便利性和舒適性，在這之中，物聯網扮演十分重要的角色，透過網路將感測器連結在一起，方能有效利用感測器所產生及蒐集的各種資料。

物聯網透過布建感測器或聯網設備蒐集大量資料，用以完善或提供各項服務。根據最新研究指出，光是智慧建築所蒐集之資料，在 2020 年就將達到 37.2 皆位元組（Zettabyte, ZB）[5]。然而，上述資料當中包含大量個人資料，根據調查顯示，近半數民眾對於個資被蒐集感到不安，希望企業能充分告知有關資料蒐集、處理及利用之目的、方式和範圍，並採取避免資料被濫用之措施[6]；更有半數以上企業認為聯網設備潛在的隱私風險將對業務和投資造成影響，使業者不敢冒然投入相關市場[7]。

有鑑於此，為進一步推動我國智慧建築發展，除調查業界在智慧建築相關之資料蒐集、處理、利用狀況及實際遭遇的困難外，亦須根據建築物類型盤點不同之資料應用情境，對應我國個資法上相關規定及司法實務，找出推動智慧建築資料應用之法制障礙，以利透過問答集等方式進行釐清，提供業界參考。

(三) 我國智慧建築門禁及安全監控設備運用現況

1. 訪談紀錄彙整

由於《建築技術規則》規範建築物之安全維護設計，故本計畫之研究範圍，亦以智慧建築之門禁系統和安全監控設備為主，合先敘明。為全面掌握上述系統和設備之現況及問題，本計畫陸續拜訪興保全、星堡保全及國霖機電等設備廠商和系統整合商，了解門禁系統和安全監控設備研發及實際導入狀況；智慧建築協會、中華民國全國建築師公會和台灣建築中心，希望能從法人和公協會角度，進一步了解業界現況和可能存在

---

3 王岫晨，〈智慧建築趨勢：綠能、感測與互聯〉，《CTIMES》，頁 48（2014）。

4 同前註，頁 49~50。

5 Xu Zheng, Zhipeng Cai, and Yingshu Li, D*ata Linkage in Smart Internet of Things Systems: A Consideration from a Privacy Perspective*, IEEE Communications Magazine, Volume56, Issue 9, *55-61(2018).*

6 ZDNet Japan，〈IoT や AI に対して不安「個人特定」「情報漏えい」--忘れられる権利を希望-日立調査〉，https://japan.zdnet.com/article/35094097/（最後瀏覽日期：109/06/16）。

7 ZDNet Japan，〈IoT のセキュリティに不安を感じる企業は半数以上-ForeScout の調査結果〉，https://japan.zdnet.com/article/35110195/（最後瀏覽日期：109/06/16）。

的法制障礙，以及對問答集的建議；最後，由於台北市政府近年建置公共住宅，導入相關智慧化系統，故本計畫亦拜訪台北市政府都市發展局住宅工程科及住宅服務科，希望了解建置過程和服務提供過程中的問題（訪談提綱及紀錄請參考附件一～附件七）。

根據訪談結果，可知目前門禁系統主要有刷卡、指紋辨識、虹膜和人臉辨識等類型，惟指紋辨識、虹模辨識因為成本太高，而人臉辨識牽涉到個資和隱私問題，故較少應用在國內社區，國內社區門禁系統仍以刷卡為主，其中感應扣是最常見的類型[8]。以台北市公共住宅為例，其門禁系統結合物業管理系統和中央監控系統，進行人員進出管制，並與消防系統連動，以便發生火災時能即時啟動消防通道和安全門，讀卡機亦具備反脅迫警報功能，可透過系統直接提供給中央監控室報警[9]。

圖 2-1 台北市公共住宅門禁系統示意圖

資料來源：台北市政府公共住宅智慧社區建置參考手冊

在監控系統方面，主要分為監視器和設備監控兩種，前者包括純影像拍攝、動態偵測和熱感應等類型，後者則是監控建築物內設備運轉狀況[10]。

8 計畫團隊親自訪談徐春福執行長、張鎧強經理，國霖機電，台中市（2020/03/31）。

9 台北市政府，《台北市政府公共住宅智慧社區建置參考手冊》，頁 22-24（2018）。

10 前揭註 8。

以台北市公共住宅為例，在設備監控上，其將建築物內之重要設備納入監控自動化系統，以監控及管制各種設備狀況，防止不當使用和意外事故發生，並將各系統之監視監控及相關信號傳至社區總管理中心，以利管理人員掌控社區資訊[11]；在監視器上，公共住宅設計以《建築技術規則》為基準，並依照住戶需求增設監視器，惟監視器拍攝區域均為公共區域，不涉及各住宅單元[12]。

公共住宅之監視系統包含：室內外網路攝影機、全功能攝影機、錄影儲存設備 NVR 及影像管理平台 CMS 軟體，並與防盜報警系統、門禁管理系統連動，設置位置則包括地下室停車場、1 樓進出口、戶外景觀或屋頂露台、各樓層梯廳、電梯、頂樓及重要機房（如中控室等）[13]。

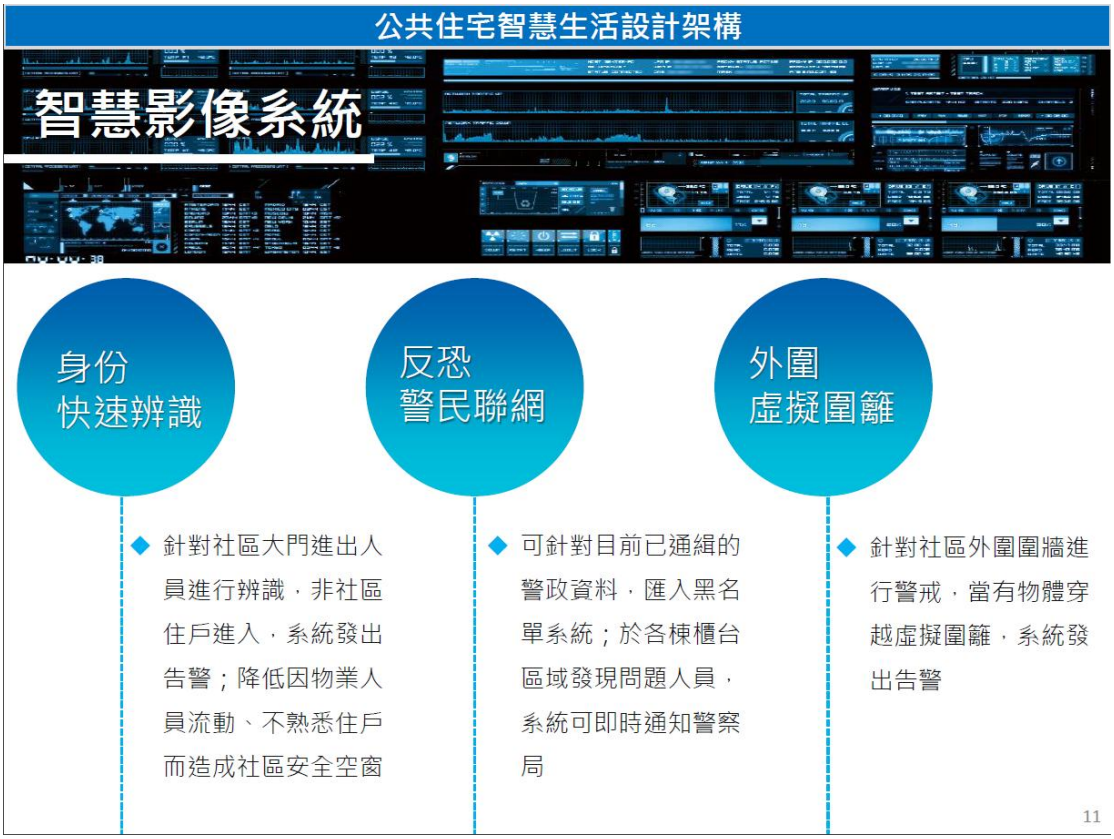


圖 2-2 公共住宅智慧影像示意圖

資料來源：台北市政府公共住宅智慧社區建置參考手冊

上述系統會蒐集大量資料，其中包括個人資料在內。以監控系統為例，雖然設備監控系統係監控建築物內設備運轉狀況，故不會蒐集到個資，

11 前揭註 9，頁 29。

12 計畫團隊親自訪談吳逸民股長、沈珮綺科員、黃慧苓科員、張裕隆正工程司、陳立人副工程司、姜國柱科員，台北市政府都市發展局，台北市（2020/05/22）。

13 前揭註 9，頁 20-21。

但監視器則會蒐集到影像資料和 IP 位址等個資；至於門禁系統，通常會蒐集使用人姓名（持卡人）、職稱、住家電話、行動電話、地址、身分證字號、統一編號、戶別、車牌和車位、出入時間和進出次數等資料，惟每間保全或物業公司設定的欄位不同，依照不同需求，有可能蒐集其他個人資料[14]。安全監視裝置所拍攝到之資料，可能有兩者用途，第一種是單純拍攝、紀錄場域狀況，以便即時發現問題（如有可疑人士進入等），第二種則是將所拍攝之資料進一步分析、利用[15]。

根據訪談結果，門禁系統及監控設備所蒐集之個人資料，未來都有進一步利用之需求，如台北市政府擬分析門禁資料以優化服務、中興保全希望能將影像資料用於機器學習，亦有受訪者分享結合門禁系統與安全監控設備資料，掌握建築物內人物動線之技術[16]。以台北市政府而言，由於上述作法均需蒐集個人資料，加上後續有進一步利用規劃，故台北市政府會與住戶簽訂契約，清楚說明個資蒐集、處理、利用方式，並會依照未來新增的利用需求進行調整，惟目前仍無向第三者提供上述資料之規劃[17]。

除上述門禁和監控系統實際運用狀況外，受訪者亦分享有關智慧建築資料應用之問題。首先，對於系統開發商而言，有利用影像資料訓練人工智慧模型之需求，惟監視器所產生之資料屬於建築物所有人、管委會等資料所有權人，廠商僅係依據代管契約保存相關資料，無法利用並發揮資料價值；資料所有權人可能會因為不確定系爭資料是否為個資，或因取得當事人同意不易而不願提供資料，就算其願意提供資料給廠商，但對系統開發商而言，亦無法確定系爭資料是否均妥善取得被拍攝之個人同意[18]。

其次，由於門禁或監控系統所生資料，大多是由保全業者或物業等進行代管，故如何監督業者落實個資法所要求之安全維護措施，成為需要關注之問題[19]；此外，在資料利用上，真正的資料所有權人亦難以利用資料，相關資料可能因為更換業者而無法使用，或受限於系統規格等原因，導致綁標狀況發生[20]；若當事人主張刪除或停止利用其個人資料的話，如原先蒐集資料是為管理場域進出狀況，則在刪除進出資料後，有可能會影響上述目的之實現，以及後續將資料進一步利用之可能性[21]。

最後，在使用者端部份，根據台北市政府說明，目前尚未接到住戶提出有關個資之客訴，在監視器等設備方面，甚至會有住戶要求在法規以外

14 計畫團隊親自訪談張順轅法務專員，台灣星堡保全股份有限公司，台南市（2020/04/01）。
15 計畫團隊親自訪談王冠翔組長，台灣建築中心，台北市（2020/09/11）。
16 前揭註 12；前揭註 15；計畫團隊親自訪談練文旭協理，中興保全，台北市（2020/03/05）。
17 前揭註 12。
18 前揭註 16。
19 前揭註 14。
20 前揭註 8；計畫團隊親自訪談溫琇玲名譽理事長，台灣智慧建築協會，台北市（2020/03/23）。
21 前揭註 16。

地方裝設[22]；惟大樓住戶或員工等特定民眾，因住在社區或在大樓內工作之故，本來就較容易取得其個資利用之同意，不易產生後續糾紛，但大樓訪客或商店顧客等難以特定之群體，就很難確保對其履行個資法相關規定[23]。從建築師角度出發，因目前智慧建築尚未法制化，故在設計智慧建築時，主要仍係依照《建築技術規則》和《智慧建築設計技術規範》進行設計，如想要求建築師落實個資和隱私保護設計於建築物，也只能透過上述規範為之[24]。惟從實務工作角度來看，目前法規密度已經足夠，規定太細反而會有難以落實的困擾[25]。

2. 國內門禁系統及安全監控設備之應用案例

根據訪談結果，綜整國內門禁系統和安全監控設備之應用案例如下：

(1) 管理人員進出、紀錄出缺勤狀況

國內門禁系統廣泛運用於社區、辦公大樓、廠房等處所，其適用之對象包括：住戶、員工或訪客。目前門禁系統主要應用方式有刷卡、指紋辨識、虹膜和人臉辨識等類型，其中感應扣或門禁卡為常見之身份驗證方式。為進行身份驗證，通常必須先取得當事人資料，方能登錄進系統，在系統中進行比對，允許符合資格者進入管制區域，其所需資料可能包括：使用人姓名（持卡人）、職稱、住家電話、行動電話、地址、身分證字號、統一編號、戶別、員工證號、車牌和車位等。

除管控人員進出特定區域外，當事人在通過門禁系統時，系統可以紀錄特定人通過時間和次數，這些資料對於公司而言，可以作為員工出缺勤紀錄[26]。

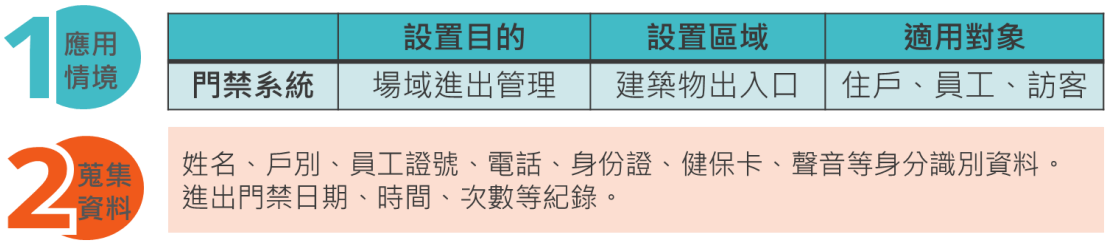


圖 2-3 門禁系統應用情境（一）

資料來源：計畫團隊自行整理

22 前揭註 12。
23 前揭註 16。
24 計畫團隊親自訪談鄭宜平理事長，中華民國全國建築師公會，台北市（2020/06/08）。
25 同前註；前揭註 12。
26 前揭註 16。

1 應用情境

	設置目的	設置區域	適用對象
門禁系統	出缺勤紀錄	辦公室門口	員工

2 蒐集資料

姓名、員工證號等身分識別資料。
進出門禁時間、次數等紀錄。

圖 2-4 門禁系統應用情境（二）

資料來源：計畫團隊自行整理

(2) 門禁系統結合其他系統提供或優化服務

門禁系統所蒐集之資料，可以進一步與監控系統、消防系統等結合，於可疑人士進入特定區域時通知保全或警消單位；或加以分析後用於優化各項管理服務，如社區管理單位分析獨居高齡者每日進出大門時間和次數，當其長時間未出現或沒有依照往常時間進出時，物業便可前往關切，了解住戶是否發生需要協助的狀況[27]。

另外，部份設有門禁系統之辦公大樓，可能會透過分析訪客在幾點幾分通過門禁系統之資料，推算出訪客會在什麼時候抵達目的地，以便安排人力在該地點等待[28]。

1 應用情境

	設置目的	設置區域	適用對象
門禁系統	優化或提供服務	建築物出入口	住戶、員工、訪客

2 蒐集資料

姓名、戶別、員工證號、電話、身份證、健保卡、聲音等身分識別資料。
進出門禁日期、時間、次數等紀錄。

圖 2-5 門禁系統應用情境（三）

資料來源：計畫團隊自行整理

(3) 透過安全監控設備監控場域狀況

建築物內會透過安全監控設備監控場域狀況，主要分成設備監控和人員監控，前者監控及管制各種設備狀況，防止不當使用和意外事故發生，後者則是透過監視器等設備拍攝特定區域，以掌握該區域內狀況。因本計畫為資料應用之研究，故研究對象以人員監控為

27 前揭註 12。
28 詳細可參考附錄十一座談會議紀錄。

主。

在人員監控狀況下，監視器通常會依照《建築技術規則》設置在公共區域，以即時監控並紀錄場域內狀況。

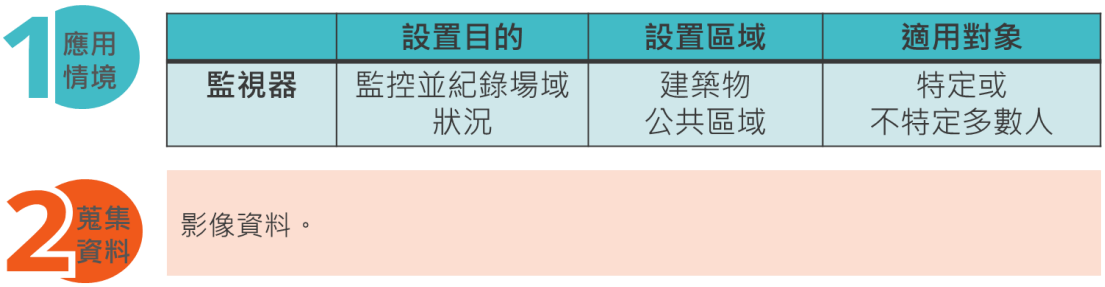


圖 2-6 安全監控設備應用情境（一）

資料來源：計畫團隊自行整理

(4) 分析安全監控設備拍攝之影像資料

監視器除用於紀錄或監控場域狀況外，其所拍攝到之影像資料，還可進一步加以利用，如保全公司分析影像資料用於訓練人工智慧[29]；店家分析影像資料統計人流和購物動線，用於改善商品上架陳列位置和結帳服務等[30]。

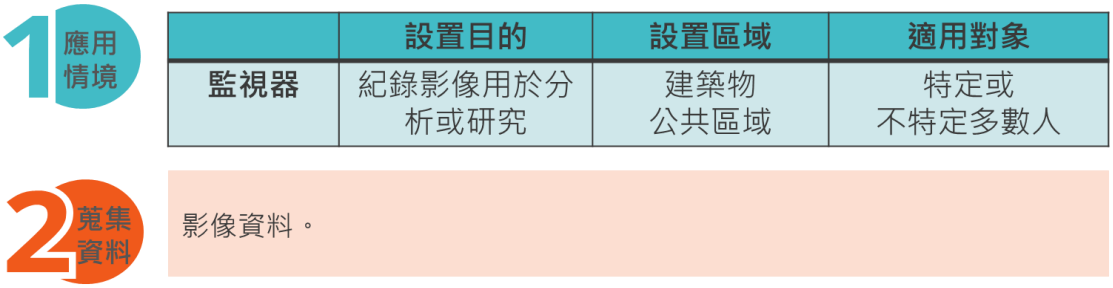


圖 2-7 安全監控設備應用情境（二）

資料來源：計畫團隊自行整理

(5) 將門禁系統和安全監控設備之資料提供給第三方

檢調單位因辦案需求，可能會向建築物所有人或場域管理單位要求

29 前揭註 16。
30 前揭註 15。

提供門禁系統和安全監控設備之資料[31]；此外，其他單位亦有可能出於研究或開發產品需求，而向建築物所有人或場域管理單位購買相關資料[32]。惟通常在設置門禁系統或安全監控設備時，不是以向第三者提供資料為目的而設置，故向第三者提供資料已經超出原先設置之目的。如果所蒐集之資料涉及個人資料，需要檢視是否符合《個人資料保護法》第 16 條或第 20 條規定，否則不能將個人資料做目的外之利用。

3. 從應用案例出發分析資料取得及利用之合法性

(1) 管理人員進出、紀錄出缺勤狀況

公司在辦公室進出口設置門禁系統，通常是為管理特定場域之進狀況，而要達到上述目的，可能會需要事先蒐集當事人資料，然後將資料處理後儲存於伺服器內，等待當事人通過門禁系統時，再與當事人所持有之門禁卡、磁扣，或輸入之密碼、指紋等資料進行比對，驗證當事人身份。

事實上，如果只是要單純管理場域進出狀況，不一定會需要蒐集當事人資料，如持有特定卡片或磁扣的狀況下，當事人只要感應卡片或磁扣就可以進入特定區域。有時候蒐集當事人資料，是為與進出時間和次數等通過門禁系統時會留下的資料進行比對，作為出缺勤紀錄。換言之，門禁系統蒐集資料之目的，其實並不僅限於場域進出管理，可能還包含其他目的。由於個資法規定在蒐集資料時需要告知當事人蒐集單位、利用目的、方式和範圍，且未來利用上述資料時，不能逾越原先蒐集時告知之目的，故若門禁系統蒐集當事人資料有管理場域進出以外之目的，建議最好能一併告知當事人。

由於門禁系統所蒐集之資料，可以直接或間接用於識別該個人，原則上均為個人資料，蒐集時應告知當事人蒐集單位、利用目的、方式、範圍等應告知事項，且在蒐集、處理時需要符合特定目的和特定情形。

然而我國個資法規定，在符合一定情況下，在蒐集資料時亦可不用告知當事人，或可在原先目的外利用資料。以公司設置門禁系統為例，公司通常會與當事人（員工）間有契約或類似契約關係，如果這些資料只是用於驗證身份或紀錄出缺勤狀況，並非出於營利考量而蒐集，且對當事人無不利影響的話，理論上不用再特別告知當事。如果沒有符合任何例外狀況，公司也可以透過取得當事人處理和利

31 〈中秋連假不打烊 警調閱監視器幫民眾找回手機〉，PChome 新聞，2020/10/06，https://news.pchome.com.tw/society/taiwanhot/20201006/index-60197913026973221002.html（最後瀏覽日期：2020/10/06）。

32 前揭註 20。

用個人資料之同意方式，蒐集、處理、利用當事人個資。

(2) 門禁系統結合其他系統提供或優化服務

集合式住宅之住戶通過門禁系統時，系統會留下通過時間和次數等紀錄，這些紀錄雖然不是可以直接用於識別個人之資料，但這些資料可以呈現出一個人日常生活的軌跡，再與其它資料結合後，若足以用於識別出特定個人，仍然有可能被認為是個人資料。

由於上述資料可能是個人資料，故想要利用上述資料，結合其他系統或進行分析以提供或改善原有服務時，都應注意符合個資法規定。在蒐集個人資料時，原則上需要告知當事人蒐集單位、利用目的、方式、範圍等應告知事項，惟若蒐集資料並非出於營利考量或對當事人有不利影響等因素，則不用特別告知當事人。另外，在蒐集和處理個人資料時應符合特定目的和特定情形。門禁系統紀錄上述資料，如果是為改善或提供管理服務，可能符合「場域進出安全管理」、「不動產服務」或「消費者、客戶管理與服務」等特定目的；若當事人與管委會、公寓大廈管理服務業者之間有契約或類似契約關係，則亦有可能符合特定情形之要求。

最後，在個人資料之利用上，必須要注意利用時須符合蒐集時之目的，如果逾越原先蒐集時之目的，則應取得當事人同意。

(3) 分析安全監控設備拍攝之影像資料

設置在公共區域之監視攝影系統，如果拍攝到足以辨識特定個人之影像或特徵，如臉上的疤痕、走路姿勢、體型等，則該影像資料有可能被認為是個人資料，必須根據個資法規定加以蒐集、處理、利用。保全公司或研究機構為研發產品或研究之需求，可能會想利用社區或大樓監視攝影系統所拍攝之影像，惟對社區管理單位而言，設置監視攝影系統只是為了監控場域內狀況，將影像資料提供或販售給第三人使用，已經逾越原先蒐集之目的，故需要檢查是否符合個資法第 20 條之例外或取得當事人同意。

承上，假使監視攝影系統拍攝到之影像，單純只有拍到風景，或雖然有拍到人物影像，卻沒有清楚拍到臉部或其他足以辨識的特徵，沒有辦法僅從影像就識別出該人身份，則該影像資料並非個人資料，利用時不會受到限制。

此外，商店內監視攝影系統所拍攝之影像資料，經分析後可以得到很多資訊，如擷取影像資料中人物特徵（性別、體型、年齡等）後，將這些資料進一步整理和歸納，可以知道來店顧客之年齡和性別組成，商店便可據此針對特定年齡、性別或體型（如服裝店）之顧客進貨；此外，商店也可以分析影像中人流動線，根據分析結果改善店內陳設和結帳動線。

針對上述原始之影像資料或人物動線資料，如果可以根據影像或動線辨識出特定人，掌握個人日常行動軌跡，則上開資料為個人資料，在蒐集、處理、利用上述資料都應遵守個資法規定。由於分析影像或人物動線和一般商店內設置監視攝影系統之目的不同，且顧客無法僅從外觀得知拍攝目的、利用方式、範圍和期間等事項，故建議店家在蒐集上述可能是個人資料之影像時，仍需透過張貼告示、廣播等方式告知當事人，並遵守個資法規定加以處理和利用。

針對上述經分析、處理過後之人物特徵或統計資料，以及將人物動線轉化成座標值之資料，假使這些資料沒有辦法回溯到特定人身上，則有可能不是個人資料，在使用時不會受到個資法之限制。以統計資料為例，假使根據影像統計來店顧客之性別組成後，發現男女客人比例為 3:7，顯示顧客以女性為主。由於上開統計資料不涉及特定個人，他人也無法僅從性別比例就推出特定人資訊或與特定人連結，故不是個人資料。

(4) 將門禁系統和安全監控設備之資料提供給第三方

檢調單位可能因辦案需要，會向社區、商店或大樓調閱監視器影像和門禁進出紀錄等資料，由於這些資料可能涉及個資，故是否能直接提供給檢調單位往往讓人感到不安。

檢調單位為公務機關，跟個資法第 15 條規定，公務機關蒐集或處理個人資料應於「執行法定職務必要範圍內」，故若檢察機關係為偵辦案件而調取資料，屬於執行法定職務範圍，則可上述規定蒐集、處理個人資料。然而對於管委會而言，向檢調單位提供上述資料不在門禁系統或監視器原先蒐集目的範圍內，故必須符合個資法第 20 條規定所列之例外情形方可提供。個資法第 20 條第 1 項但書第 2 款規定：「為增進公共利益所必要」時，個人資料可以為特定目的外利用，檢察機關是為偵辦案件而調取資料，協助檢查機關辦案應符合「為增進公共利益所必要」，故應可向檢查機關提供門禁資料或監視器拍攝之影像資料。

另外要注意影像資料不一定為個人資料，以裝設在車站或百貨公司等人潮聚集處之監視器為例，拍攝到的對象為不特定多數人，無法僅從影像就可辨識出特定個人，則上述資料應非個人資料，不適用個資法（參考法務部法律字第 0999009760 號函釋）。然而若能從影像中辨識出特定個人，如監視器清楚地拍攝到人群中某人的臉部或身體特徵，與其他資料比對後可以知道對方是誰，則該影像資料仍有可能是個人資料。此外，如果監視器是裝設在社區或集合式住宅內，由於被拍攝到的民眾通常為住戶，相對容易特定身份，故有較高的可能被認定為個人資料。

綜上所述，只要拍攝到足以識別出特定個人之影像，無論是拍到當

事人正面或鏡面、玻璃窗中反射影像，都有可能為個人資料。

(四) 我國智慧建築門禁及安全監控資料應用法制障礙

1. 以問答集引導實務方向及消除灰色地帶

綜整訪談過程中所提到之門禁和監控系統實際運用狀況，個人資料蒐集、處理及利用方式和需求，以及實務上所遭遇的問題後，可發現雖然使用者不一定會對門禁和監控系統蒐集、處理、利用個資之方式提出異議，但對於有資料利用需求之廠商，或是建造、設計和提供智慧化生活服務者而言，由於對個資相關規範不太熟悉，故大多難以判斷目前所採取之措施是否符合法規要求，進而影響後續資料流通和利用。

想要解決上述問題，或許可從建築物設計或建造階段著手，要求建築師或建商設計建造符合個資法規定及落實隱私保護之建築物。針對建築物在設計建造時應落實個資法和隱私保護，我國已於《建築技術規則》第 116-1 條至第 116-7 條規定，規範建築物之公共空間應設置各項安全維護措施，並於第 116 條之 4 第 2 項規定：「設置前項裝置，應注意隱私權保護。」惟對於建築師和建商而言，究竟該如何落實第 116 條之 4 第 2 項規定？由於法條並未具體規範應採取之措施，難以檢視建築物是否有遵守此項規定，故本項規定應僅具有宣示性功用，只能提醒建造者注意避免違反《個人資料保護法》（以下簡稱個資法）或《刑法》等法規中有關個資和隱私保護之規定。

有鑑於此，應有必要進一步說明建築物在設計建造時，如何落實隱私權保護。惟需注意的是，從前述訪談內容，可知對實際設計、建造智慧建築者而言，法規太過詳細，反而會增加實務工作上困擾，無法保留日後更改設計或翻修改建之彈性；此外，詳細規範建築物設計方式或相關裝置應設置位置亦有所困難。以監視器為例，《建築技術規則》第 116-1 條以下規定安全維護裝置應設置或得設置之處所，上述處所均為公共空間，惟縱使監視器設置在公共空間，但所拍攝之影像如清楚拍到人臉或其他得識別身份之資訊，仍有可能被認定為個人資料，故無法僅依據監視器設置之場所，就可以確認拍攝到之影像是否涉及個資，從而斷定不會有個資或隱私侵害之可能。

除上述問題外，對實際使用建築物內相關安全維護措施者，如物業、保全業或建築物所有人等而言，即便知道建築物符合《建築技術規則》，但在使用相關設備時，仍然不知道是否需要告知被拍攝者有設置監視器、告知的內容，以及公共區域影像是否為個資、是否能逕行提供給第三人使用等問題。之所以會發生上述問題，其理由在於許多個資或隱私相關問題，其實與建築物如何設計或建造無關，而是與使用者是否依照個資法要求蒐集、處理、利用資料有關。

綜上所述，本文認為，想要透過清楚規範建築物設計或建造標準，來落實個資和隱私保護並不容易，加上許多使用上的問題無法透過設計解決，

故針對法規適用上曖昧不明的灰色地帶，以問答集形式加以說明，銜接法規與實務工作間的落差，或許是更好的作法。為達上述目的，本研究擬參酌歐盟、英國及日本等地區和國家作法，作為研提我國智慧建築門禁及安全監控資料應用法制相關指引之參考。

2. 促進智慧建築資料流通和利用

除上述問題外，從前述訪談結果，亦可發現智慧建築內亦存在資料所有權人和資料管理者、利用者間權利關係不明的狀況。由於真正擁有資料所有權的人，可能並未持有資料，故亦難以進一步加以利用。為促進智慧建築資料流通和利用，除透過問答集澄清法規適用上的疑義外，另外一個可能的作法，是透過立法來促進資料開放、流通和利用。以近年開放資料（open data）之立法趨勢為例，為順應大數據發展，各國政府推動開放政府機關所持有之資料，隨著政府所釋出之資料數量漸漸增長，加上對於資料數量和品質的需求不斷增加，上述開放資料之對象亦逐漸轉向民間部門所持有之資料，惟想要透過法規要求民間部門釋出所持有之資料並不容易，故大多仍是透過制定指引或提供契約範本等方式，促進民間資料之流通和利用[33]；此外，在開放的資料類型上，原先可能聚焦在不涉及個資、隱私或機密性之資料，但現在也可透過去識別化或假名化等方式，讓上開資料得以在經處理後加以利用。

因應上述立法趨勢，我國於 2015 年制定《政府資訊公開法》，便利人民共享及利用政府資訊，現在亦正研擬開放資料專法，希望能進一步透過法律規範資料開放格式、資料共享及流通等事項，加強政府資料之開放運用[34]。惟上開法律之規範主體均為政府機關，由此可知我國開放資料範圍仍以政府機關所持有之資料為主，尚未涉及民間部門所持有之資料，加上在私法自治原則下，想要透過法律介入私領域，要求私人開放資料並不容易，有鑑於此，未來或可考慮透過研擬資料契約範本，讓資料所有權人與利用者之間，可以清楚約定資料蒐集、儲存及使用權限等細節，以確保資料所有權人之權益，並提高資料所有權人提供資料之意願。

根據上述開放資料立法趨勢檢視建築領域之資料利用，本研究擬從公部門建築物和民間部門建築物之資料利用兩方面加以分析。首先，針對公部門建築物之資料利用，由於目前開放資料專法尚未公布，故本研究儘先以《政府資訊公開法》作為討論對象，合先敘明。根據《政府資訊公開法》第 5 條，政府資訊應主動公開或應人民申請提供，惟依照同法第 3 條，可知所謂政府資訊，係指『政府機關於職權範圍內作成或取得而

---

33 如日本針對產業資料之利用，制定及修正《不正競爭防止法》（不正競争防止法）、《生產力提昇特別措施法》（生產性向上特別措置法），並制定公布多部促進資料利用相關之指引。關於日本資料法制介紹，可參考：周晨蕙，〈產業資料與個人資料之加值運用法制-以日本為例〉，《科技法律透析》，第 31 卷第 9 期（2019）。

34 〈推動開放資料專法 建構資料共享新世代〉，國家發展委員會，https://www.ndc.gov.tw/News_Content.aspx?n=114AAE178CD95D4C&sms=DF717169EA26F1A3&s=0E2ADAF00CD83B6B（最後瀏覽日期：2020/09/29）。

存在於文書、圖畫、照片、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物及其他得以讀、看、聽或以技術、輔助方法理解之任何紀錄內之訊息。』故公部門建築物資料是否為政府資訊，端視其是否為政府機關於職權範圍內作成或取得而定。

政府機關於建築物內導入門禁或安全監控設備，可能是出於管理場域進出狀況或監視場域安全之目的，惟上述目的通常並非各級政府機關之法定職權範圍。此外，根據《政府資訊公開法》第 1 條，可知本法之立法目的在於『便利人民共享及公平利用政府資訊，保障人民知的權利，增進人民對公共事務之瞭解、信賴及監督，並促進民主參與』公開門禁系統所紀錄之個人資料或監視器所拍攝到之影像資料，無法達到增進人民對公共事務之瞭解、信賴及監督等目的，故公部門建築物資料應非屬政府資訊之範疇。綜上所述，在《政府資訊公開法》擴張政府資訊範圍之前，我國政府機關並無主動公開建築物資料或應民眾申請提供之義務。

其次，針對民間部門建築物之資料利用，如前所述，我國開放資料之範圍僅限於政府機關所持有之政府資訊，故民間部門建築物之資料利用，屬於私法自治的範圍，須由資料所有權人和利用者之間約定利用方式、期間和範圍。以我國公寓大廈為例，公寓大廈管理委員會為處理社區內行政事務，可能有調閱、公布或向他人提供門禁資料和監視器影像資料之需求。針對上述資料蒐集、處理和利用之需求，如能事先透過公寓大廈規約加以約定，可以避免未來管理委員會和住戶之間產生糾紛，故日後或可檢討修正公寓大廈規約範本，於範本內加入建築物資料蒐集、處理和利用等事項。

3. 推動智慧建築門禁及安全監控資料應用之應備法制

綜合前述分析，可知智慧建築門禁及安全監控資料應用主要有不清楚資料取得和利用之適法性，以及資料所有權不明，難以約定資料應用方式等問題。惟除上述問題外，為避免資料在蒐集、處理、利用過程中外洩，導致個人權利受到侵害，如果確保資料保存和傳輸過程中安全性及資料正確性，亦為後續值得探討的課題。

針對上述資料取得和利用之適法與否問題，本研究提出透過制定問答集或指引，銜接法規與實務工作間的落差之建議，並已提出問答集草案作為研究成果。惟針對研議確保資料安全和正確性之機制，以及檢討制定資料契約範本，以促進智慧建築資料流通等問題，仍有待後續研究持續加以完善。

第二節、 國外智慧建築資料應用法制及具體案例

(一) 個資保護之國際立法趨勢與我國法制現況

從上述智慧建築定義及發展趨勢，可知物聯網是實現智慧建築之重要關鍵。然而，由於在物聯網環境下，資料可以在不同資料庫之間交換、比對、分析，使原先並非個人資料之資料，在經比對後亦可辨識出特定個人，對個人資料保護和隱私權產生威脅，進而引發諸多討論，並促使各國修法以茲因應。

以歐盟為例，2013 年歐盟執委會針對物聯網提出公眾意見諮詢並研擬發展方針，歐盟資料保護工作小組於 2014 年提出報告，整理物聯網相關個資及隱私課題，如使用者難以控制其個資、難以行使同意權、對於資料推論及二次利用逸脫於原始蒐集目的外等……[35]。隨後，歐盟電子通訊管制諮詢機關（Body of European Regulators for Electronic Communications, BEREC）在 2016 年 2 月發布有關促進物聯網發展之報告（BEREC Report on enabling Internet of Things），其認為不需要針對物聯網建構新的資料保護規則，但部份規定仍有因應物聯網環境加以調整之需要，如告知和取得同意之方式等[36]。

在提出上述報告後，歐盟於 2016 年 4 月通過《一般資料保護規則》（General Data Protection Regulation, GDPR），歐盟執委會並於 2017 年提出《隱私與電子通訊規則》（Regulation on Privacy and Electronic Communications）草案，作為補充 GDPR 之規定，雖然後者迄今尚未通過，但其主要精神仍與 GDPR 方向一致[37]。有學者整理 GDPR 中與物聯網相關之規定，分別為『個資洩漏事故發生之強制通報義務、自動化設備資料主體之告知同意[38]、從設計著手保護隱私[39]，以及增進當事人權利[40]等』[41]。

由於歐盟 GDPR 施行後，其適用對象除歐盟境內設立據點的企業外，還包括對歐盟境內人民提供產品、服務或監測歐盟境內人民網路行為之境外企業；加上 GDPR 原則上禁止個資跨境傳輸，只有取得適足性認定資格之國家，才可以自由與歐盟境內進行個資跨境傳輸，故日本於 2020 年 6 月配合 GDPR 修正個資法，成為 GDPR 施行後第一個取得適足性認定之國家[42]。

---

35 葉志良，〈因應物聯網發展資料保護法制的革新-歐盟法制的發展與啟示〉，《中原財經法學》，第 40 期，頁 76（2018）。

36 同前註，頁 87。

37 前揭註 35，頁 86-87。施弘文，〈歐盟執委會提出「隱私與電子通訊規則」草案〉，《科技法律透析》，第 29 卷第 6 期，頁 4（2017）。

38 亦即 GDPR 第 21～22 條與自動化個人決定與特徵分析有關之規定。

39 原文為 Privacy by Design，亦有翻譯為設計階段納入隱私考量，可參考：徐彪豪，〈物聯網時代的資料保護防線－以歐盟 GDPR 為中心〉，《科技法律透析》，第 28 卷第 10 期，頁 4（2016）。本文於此使用原文作者翻譯，後文則統一使用「設計階段納入隱私考量」。

40 GDPR 大幅強化資料主體權利，包括被遺忘權、資料可攜權、資料自動化處理等，而這些權利均與近年物聯網對於個資保護之影響有關。關於 GDPR 立法重點介紹，可參考徐彪豪，同前註，頁 59-67。

41 前揭註 35，頁 91-98

42 〈爭取歐盟 GDPR 適足性認定 國發會：去年底已遞件〉，自由時報，2019/02/18，https://ec.ltn.com.tw/article/breakingnews/2702576（最後瀏覽日：2020/09/22）。

為配合歐盟 GDPR 施行，日本自 2019 年起檢討個資法內有關個人資料開示（第 28 條）、訂正（第 29 條）及停止利用（第 30 條）規定，比較 GDPR 第 20 條資料可攜權、第 21 條異議權及第 22 條自動化數位剖析許可權[43]，以及國際間類似規定，作為修正參考[44]。完成上述檢討後，日本內閣於 2020 年 3 月 10 日向國會提出個資法修正案，參議院則於同年 6 月 5 日通過上述修正案，以強化對個人資料之保護[45]。此次修正案重點包括：強化停止利用和刪除個人資料之權利，如企業利用個資可能侵害當事人權利時，當事人便可要求停止利用其個資；個資洩漏事故發生時之通報義務、創設介於個資和去識別化個資間之個資「假名化」制度，以及強化違反個資法規定之罰則等[46]。

綜上所述，可發現強化當事人對於個資的控制，實為近年重要之國際立法趨勢。我國於 2015 年修正《個人資料保護法》，明定蒐集、處理、利用特種個資要件，並因應近年網路和新科技發展，放寬當事人表示同意之方式，強化對於個人資料之保護，惟與歐盟 GDPR 或日本個資法相比，可發現我國並未建立獨立的個資專責機關，同時亦未在個資法內清楚定義去識別化及規範去識別化之方式，僅透過函釋說明去識別化為處理個人資料的方式之一[47]。此外，根據我國個資法第 11 條規定，當事人僅能在個資蒐集目的消失或屆滿，以及個資被違法蒐集、處理或利用等狀況下，要求停止蒐集、處理、利用或刪除個人資料，與前述日本個資法修正後，允許在利用個資可能侵害當事人權利狀況下，便可要求停止利用或刪除其個人資料相比，對於資料主體權利保障仍略有不足。

基於上述理由，我國為爭取申請 GDPR 適足性認定，近來亦積極檢討個資法，擬強化對於個資之保護[48]。惟本研究重點並非進行各國個資法之比較，以及從比較法角度出發，研提我國修法建議，而是如何落實我國個資法規定並釐清民眾對於個資和隱私之疑慮，故本報告在簡述個資法立法趨勢及進行簡單比較後，將針對歐盟、英國及日本有關個資或安全監控設備之指引進行介紹，了解上開地區及國家係如何透過指引引導實務方向，以便作為本計畫研擬問答集之參考。

---

43 關於資料可攜權、異議權及自動化數位剖析許可權等翻譯，係引用李世德，〈GDPR 與我國個人資料保護法之比較分析〉，《台灣經濟論衡》，第 16 卷第 3 期，頁 87（2018）。

44 《個人情報保護を巡る国内外の動向》，頁 8-19（2019），https://www.ppc.go.jp/aboutus/minutes/2018/20190320/（最後瀏覽日：2019/07/23）。

45 〈個人データに利用停止権、改正個人情報保護法が成立〉，日本經濟新聞，2020/06/05，https://www.nikkei.com/article/DGXMZO60009640V00C20A6MM0000/（最後瀏覽日：2020/06/09）。

46 個人情報保護委員会，〈「個人情報の保護に関する法律等の一部を改正する法律案」の閣議決定〉，2020/03/10，https://www.ppc.go.jp/news/press/2019/20200310/（最後瀏覽日：2020/06/09）。

47 國家發展委員會，〈歐盟 GDPR 與我國個人資料保護法之重點比較分析〉，https://www.ndc.gov.tw/Content_List.aspx?n=92A54D2FBC1D329E（最後瀏覽日期：2020/10/06）。

48 前揭註 42。

(二) 歐盟個人資料保護相關指引

1. 歐盟 IT 治理與 IT 管理之個人資料保護指引

根據歐盟第 45/20013/EC 號規則（Regulation (EC) No 45/2001），為協助歐盟機構和組織設計及落實內部控制機制（internal control system）和 IT 治理，歐盟資料保護監督機關（European Data Protection Supervisor, EDPS）制定「歐盟 IT 治理與 IT 管理之個人資料保護指引」（Guidelines on the protection of personal data in IT governance and IT management of EU institutions），以確保歐盟機構在處理個人資料時遵守「設計階段納入隱私考量」，和「預設隱私設定」（privacy by default）等規範[49]。

本指引分為 5 章，第 1 章為目的；第 2 章為指引範圍和架構說明；第 3 章為 IT 治理和 IT 管理之定義；第 4 章為介紹個資保護法律框架，以及在整個資訊系統生命週期中應注意之個資保護原則；第 5 章為如何將個資保護要求落實到資訊系統生命週期內之說明。

根據指引第 3 章說明，IT 治理和 IT 管理為組織之核心功能，用於確保組織之 IT 環境與目標保持一致，前者為戰略層面（要做什麼），後者則為戰術層面（如何做）之概念，而為落實 IT 治理，其架構和流程設計應符合資料保護原則，範圍則應涵蓋組織和員工規範，如明確定義各人職責，以及提高員工對於個資保護之認識[50]。

在介紹基本概念後，本指引於第 4 章介紹第 45/20013/EC 號規則和一般個人資料保護規則（General Data Protection Regulation, GDPR）等規範，並以列出應遵守之個資保護要求，包括（1）合法、公平及透明性；（2）目的限制：僅能在具有明確且合法目的前提下處理個人資料；（3）資料最小化：（4）準確性；（5）儲存限制：如儲存時間不得超過達成目的所需時間、保留期間與收集目的成比例等；（6）誠信與保密：採取確保個資安全性之措施；（7）問責制：確保符合上述原則[51]。

最後，第 5 章針對整個 IT 系統生命週期之個資處理進行說明，並於附件以表格方式，整理 IT 系統各階段應注意事項。

表 2-2 IT 系統生命週期各階段之個資保護建議

生命週期	流程	建議	一般性建議
開始階段		確定系統所處理之資料是否為個人資料，或	IT 系統所有階段均應遵守個

[49] European Data Protection Supervisor, *Guidelines on the protection of personal data in IT governance and IT management of EU institutions*, 2018/03/23, p.4, https://edps.europa.eu/data-protection/our-work/publications/guidelines/it-governance-and-it-management_en (last visited 2020/06/03).

[50] *id* at p.7-11.

[51] *id* at p.12-15.

		經過處理後可成為個人資料	資保護原則
		規則內應包含高等級之個資保護要求	
發展階段	蒐集要求	應從利益相關者蒐集資料保護要求，並將其紀錄於系統	
	設計	應針對敏感性之個資採取額外防護措施	
		設計時應預留充分時間以執行後續操作，如匿名處理和刪除資料	
過度與部屬階段		系統終端用戶、管理員和維護人員應充分了解個資保護規範	
操作&維護階段		所有透過系統處理之個資均需向組織內資料保護人員註冊。	
		應確認資料可儲存之時間，以確保其符合相關規定。	
	資料主體資訊和透明度	組織應建立可適時通知操作資訊和使用資訊之管道，使資料主體可以獲取資訊	
	登入管理	建立用戶管理和許可程序，如系統訪問權限	
	變更管理	建立正式變更程序，統一處理所有變更申請	
	安全監控	持續監控對個資之訪問（access）	
	資料交換	只能在安全管道（如加密）傳輸個資	
		使用電子郵件等方式傳輸個人資料，應了解這些技術既有問題，並將問題反應於風險評估中，如透過加密郵件進行傳輸	
	處理方式	應建立確保資料移轉時滿足個資保護要求之程序	
橫向階段	採購流程	契約等文件應包括承	

		包商應採取之技術和措施，以確保對個資之保護	
	專案管理	管理者應與個資保護負責人保持聯繫	
	治理	管理層應明確支持個資保護原則	
		高階管理人員應對個資保護負責	
		高階管理人員應對負責個資保護，或指定負責人員	
		所有員工均應了解有關個資保護之政策與程序	
		定期檢視和維護個資保護政策	
		讓審計人員參與內部控制機制之評估	

資料來源：Guidelines on the protection of personal data in IT governance and IT management of EU institutions

2. 監視器影像個人資料處理指引 3/2019

鑑於監視器設備和影像之使用對個人資料保護和隱私之影響，以及臉部辨識影像潛藏的歧視風險等問題，歐盟資料保護委員會（European Data Protection Board, EDPB）於 2019 年 7 月 10 日公布「監視器影像個人資料處理指引 3/2019」（Guidelines 3/2019 on processing of personal data through video devices），說明如何在符合 GDPR 規範下處理個人資料，並在公布上開指引後，又於 2020 年 1 月 29 日修正公步第二版指引[52]。

「監視器影像個人資料處理指引 3/2019」強調監視器影像資料之利用，必須避免目的外利用，且管理者應仔細考量 GDPR 第 5 條有關監視器之規範，並採取適當之預防措施，防止設備故障及潛在的風險等，並針對監視器處理個人資料之合法性、資料主體權利、個資儲存和刪除等常見問題加以說明。

本指引一共分為 10 章，第 1 章說明指引制定目的；第 2 章說明指引範圍

52 European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video device*, 2020/01/30, p.5-6, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en (last visited 2020/06/04).

包括個人資料及歐盟第 2016/680 號指令（Directive 2016/680），第 2016/680 號指令為歐盟於 2016 年 4 月 27 日公布，有關主管機關以預防、偵查或起訴刑事犯罪或執行刑罰為目的處理個人資料之法規。必須注意的是，雖然根據 GDPR 規定，在單純的個人或家庭活動中處理個人資料，並非 GDPR 所欲規範之行為，惟在使用監視器狀況下，上述有關家庭豁免（Household exemption）之規定必須以狹義方式加以詮釋，僅限於與私人或家庭活動過程中有關之行為[53]。此外，即便是在公共空間，如監視系統不斷紀錄與儲存個人資料，此種行為亦無法被認為是單純的個人或家庭活動，從而免除 GDPR 之適用[54]。

第 3 章說明處理個資之合法性要件，如使用前必須詳細說明使用目的，如使用監視器之目的是為避免財產遭竊，以及符合最小化原則，並且在個案中考量目的與手段（使用監視器）間之關係，確保利益衡平，以及滿足個人對於個資利用之合理期待；第 4 章以下則陸續就將公開或向第三方披露影像必須具備法律依據並採取適當措施、特別資料之處理、資料主體權利（請求刪除和告知當事人方式）、資料透明性、儲存期限、技術及組織規範（在設計規範中納入隱私考量）、資料保護衝擊評估等議題加以說明，使民眾得以理解如何落實 GDPR 於監視器影像資料之處理。

(三) 日本個人資料保護相關指引

1. 網路安全相關法令 Q&A 手冊

日本內閣於 2017 年 7 月 27 日通過「網路安全戰略」（サイバーセキュリティ戦略），其中提到應整理相關法制，以利業者參考實行網路安全對策，故內閣網路安全戰略本部普及啟發·人才培育專門調查會（サイバーセキュリティ戦略本部普及啓発・人材育成専門調査会）於同年 10 月 10 日成立工作小組，推動網路安全相關法令調查工作[55]。工作小組以經產省於 2008 年公布之「資訊安全相關法令要求事項集」（情報セキュリティ関連法令の要求事項集）為基礎，根據近年情勢和相關法令變化，增加企業網路安全對策等內容，檢討制定「網路安全相關法令 Q&A 手冊」（サイバーセキュリティ関係法令 Q&A ハンドブック），該手冊最終於 2020 年 3 月 2 日正式於網站上公布[56]。

在 2013 年制定《網路安全基本法》（サイバーセキュリティ基本法）之前，日本法上並無網路安全（サイバーセキュリティ）概念，甚至沒有「安全」（セキュリティ）等用語，唯一近似的概念為 2000 年所制定之 IT 基本法第 22 條所提到之「高度資通訊網路安全性及信賴性」，可將

53 *id* at p.7.
54 *id*
55 內閣サイバーセキュリティセンター，〈サイバーセキュリティ関係法令Q&Aハンドブック作成・公開のお知らせ〉，2020/03/02，https://www.nisc.go.jp/security-site/files/lawhandbook_press.pdf（最後瀏覽日期：2020/05/28）。
56 同前註。

之解釋為包含資訊機密性（Confidentiality）、完整性（Integrity）及可用性（Availability）等三要素之資訊安全[57]。在 2013 年制定通過《網路安全基本法》後，該法從資訊、資訊系統和資通訊網路三大面向定義網路安全，並規範日本國內網路安全政策框架及對企業之權利和義務等事項，惟仍缺乏可作為通則適用於企業之網路安全權利及義務相關法令，加上個別法律中亦有網路安全相關規定，故日本政府方才透過制定手冊，提供企業作為實施具體資安對策之參考[58]。

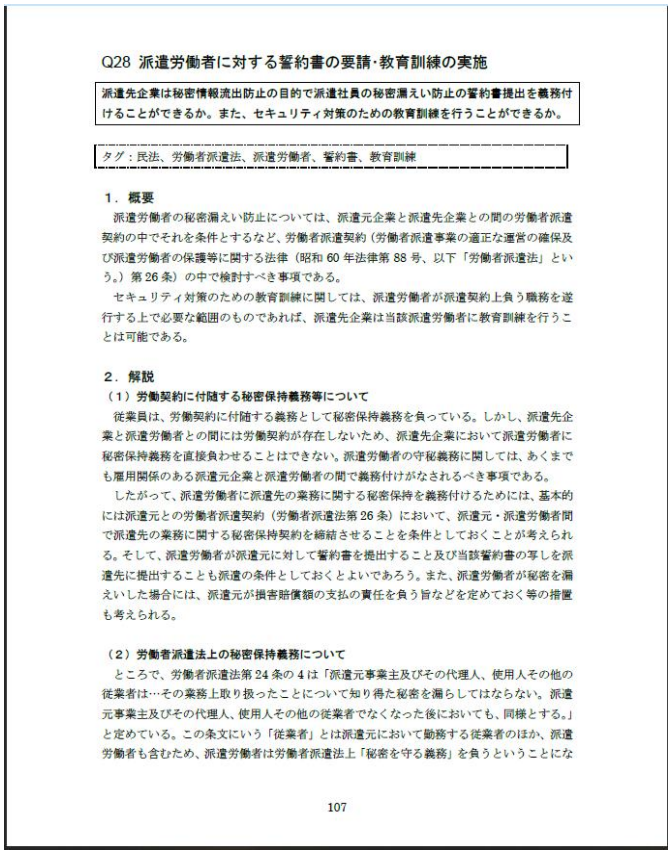
「網路安全相關法令 Q&A 手冊」內所提到之法律包括：網路安全基本法、民法、公司法、個人資料保護法、不正競爭防止法、著作權法、勞動基準法、電力通信事業法、電子簽章及認證法、促進資訊處理法、國立研究開發法人資通訊研究機構法、刑法和禁止以不正方式連接法等。手冊內蒐錄 73 個 Q&A，Q1、2 為說明網路安全基本法概要及網路安全概念；Q3~Q6 以公司法為中心，從經營觀點出發說明董事義務（建立內控機制）；Q7~Q16 以個資法為中心，說明個資安全管理措施、信用卡資訊、勞工身心狀態資訊等；Q17~Q22 以不正競爭防止法為中心，說明營業祕密保護、限定提供資料等概念；Q23~Q35 以不正競爭防止勞動法為中心，說明企業實施資安對策時，組織及員工相關對策；Q36~Q38 以資通訊網路、電信業者等為中心，說明 IoT 相關法律問題；Q39~Q43 以契約關係為中心，說明電子簽章、資料交易、系統開發、雲端服務等議題；Q44~Q45 網路安全相關證照制度（如資訊處理安全確保支援士）；Q46~Q49 說明其他網路安全議題，如密碼、資訊共享、輸出管理等；Q50~Q58 說明網路安全相關事件發生後之因應措施（如數位鑑識等）；Q59~Q64 說明網路安全相關之民事糾紛；Q65~Q71 網路安全相關之刑法問題；Q72~Q73 我國業者應注意之外國網路安全規範[59]。

在具體 Q&A 的編排上，手冊大致上將每個問題分為(1)概要(2)詳細說明(3)相關法令(4)相關判例等 4 個部份，如下圖所示。

57 内閣サイバーセキュリティセンター，《サイバーセキュリティ関係法令 Q&A ハンドブック》，頁 1（2020）。

58 同前註，頁 2。

59 同前註，頁 4。



Q28 派遣労働者に対する誓約書の要請・教育訓練の実施

派遣先企業は秘密情報流出防止の目的で派遣社員の秘密漏えい防止の誓約書提出を義務付けることができるか。また、セキュリティ対策のための教育訓練を行うことができるか。

タグ：民法、労働者派遣法、派遣労働者、誓約書、教育訓練

1．概要

派遣労働者の秘密漏えい防止については、派遣元企業と派遣先企業との間の労働者派遣契約の中でそれを条件とするなど、労働者派遣契約（労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律（昭和 60 年法律第 88 号、以下「労働者派遣法」という。）第 26 条）の中で検討すべき事項である。

セキュリティ対策のための教育訓練に関しては、派遣労働者が派遣契約上負う職務を遂行する上で必要な範囲のものであれば、派遣先企業は当該派遣労働者に教育訓練を行うことは可能である。

2．解説

（1）労働契約に付随する秘密保持義務等について

従業員は、労働契約に付随する義務として秘密保持義務を負っている。しかし、派遣先企業と派遣労働者との間には労働契約が存在しないため、派遣先企業において派遣労働者に秘密保持義務を直接負わせることはできない。派遣労働者の守秘義務に関しては、あくまでも雇用関係のある派遣元企業と派遣労働者の間で義務付けがなされるべき事項である。

したがって、派遣労働者に派遣先の業務に関する秘密保持を義務付けるためには、基本的には派遣元との労働者派遣契約（労働者派遣法第 26 条）において、派遣元・派遣労働者間で派遣先の業務に関する秘密保持契約を締結させることを条件としておくことが考えられる。そして、派遣労働者が派遣元に対して誓約書を提出すること及び当該誓約書の写しを派遣先に提出することも派遣の条件としておくとよいであろう。また、派遣労働者が秘密を漏えいした場合には、派遣元が損害賠償額の支払の責任を負う旨などを定めておく等の措置も考えられる。

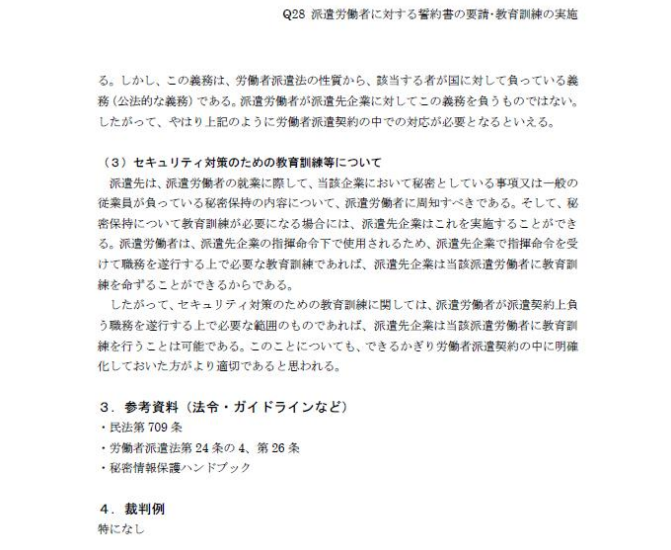
（2）労働者派遣法上の秘密保持義務について

ところで、労働者派遣法第 24 条の 4 は「派遣元事業主及びその代理人、使用人その他の従業者は…その業務上取り扱ったことについて知り得た秘密を漏らしてはならない。派遣元事業主及びその代理人、使用人その他の従業者でなくなった後においても、同様とする。」と定めている。この条文にいう「従業者」とは派遣元において勤務する従業者のほか、派遣労働者も含むため、派遣労働者は労働者派遣法上「秘密を守る義務」を負うということにな

107

圖 2-8 網路安全相關法令 Q&A 手冊內頁（1）

資料來源：サイバーセキュリティ関係法令 Q&A ハンドブッ



る。しかし、この義務は、労働者派遣法の性質から、該当する者が国に対して負っている義務（公法的な義務）である。派遣労働者が派遣先企業に対してこの義務を負うものではない。したがって、やはり上記のように労働者派遣契約の中での対応が必要となるといえる。

（3）セキュリティ対策のための教育訓練等について

派遣先は、派遣労働者の就業に際して、当該企業において秘密としている事項又は一般の従業員が負っている秘密保持の内容について、派遣労働者に周知すべきである。そして、秘密保持について教育訓練が必要になる場合には、派遣先企業はこれを実施することができる。派遣労働者は、派遣先企業の指揮命令下で使用されるため、派遣先企業で指揮命令を受けて職務を遂行する上で必要な教育訓練であれば、派遣先企業は当該派遣労働者に教育訓練を命ずることができるからである。

したがって、セキュリティ対策のための教育訓練に関しては、派遣労働者が派遣契約上負う職務を遂行する上で必要な範囲のものであれば、派遣先企業は当該派遣労働者に教育訓練を行うことは可能である。このことについても、できるかぎり労働者派遣契約の中に明確化しておいた方がより適切であると思われる。

3．参考資料（法令・ガイドラインなど）

・民法第 709 条
・労働者派遣法第 24 条の 4、第 26 条
・秘密情報保護ハンドブック

4．裁判例

特になし

圖 2-9 網路安全相關法令 Q&A 手冊內頁（2）

資料來源：サイバーセキュリティ関係法令 Q&A ハンドブッ

2. 監視器影像指引及案例集

日本 IoT 推動協議會、經產省和總務省鑑於業者設置監視器之需求，針對監視器特性（被拍攝人無法於事前被告知；從攝影機外觀難以得知後續利用方式等），組成工作小組，從實際運用情境出發，檢討向一般人告知監視器存在及拍攝影像利用目的等方式，於 2017 年 1 月公布「監視器影像加值運用指引第 1 版」（カメラ画像利活用ガイドブック ver1.0），隨後以上述指針內容為基礎，增加新的運用情境後，在 2018 年 3 月公布「監視器影像加值運用指引第 2 版」（カメラ画像利活用ガイドブック ver2.0），其內容包括事前告知、取得、處理及管理影像之基本原則，以及實際運用案例說明[60]。上開指引雖無強制力，但日本政府希望可以藉由本指引之說明，作為業界利用監視器影像之框架規範。

工作小組整理監視器影像之運用方式和拍攝對象、場所如下表：

表 2-3 監視器影像運用方式與案例

No	分類	案例
1	不識別特定個人，僅利用風景影像等資料	掌握道路變化等資料，用於更新地圖資訊
2	統計人數作為統計資料	掌握通行人數，用於擬定都市計畫
3	分析人物屬性作為統計資料	掌握性別與年齡組成等資訊，用於開發商品
4	取得座標等動線資料，作為統計資料	掌握人流移動與滯留狀況，或人流在商品陳列架前之行動等資訊，規劃商店動線或商品陳列方式
5	取得特定個人於一定期間之來店履歷、動線資料、購買履歷以及性別、年齡，作為統計資料	分析來店履歷、行動履歷、購買履歷以及人物屬性之間的關聯性，以調整販售商品種類使其符合客人興趣，或打造最佳動線及商品陳列方式
6	將影像資料與會員資料等進行比對，作為市場	掌握個人的購買履歷或行動履歷，用於提供個人化服務

60 〈「カメラ画像利活用ガイドブック ver2.0」を策定しました〉，經濟產業省，https://www.meti.go.jp/press/2017/03/20180330005/20180330005.html（最後瀏覽日期：2020/10/06）。

	行銷資料	

資料來源：カメラ画像利活用ガイドブック ver2.0

表 2-4 監視器拍攝場所

No	分類		案例
1	公開空間（無明確的入口或動線）	公共空間	道路、公園等
		準公共空間	車站內（閘門外）、店舖前等
2	私人空間（以入口或閘門明確區分區域內外）	特定空間	店舖內或設施內等

資料來源：カメラ画像利活用ガイドブック ver2.0

根據上述監視器影像利用方式和拍攝場所，工作小組劃定「監視器影像加值運用指引」檢討範圍如下圖，並針對具體案例進行說明。

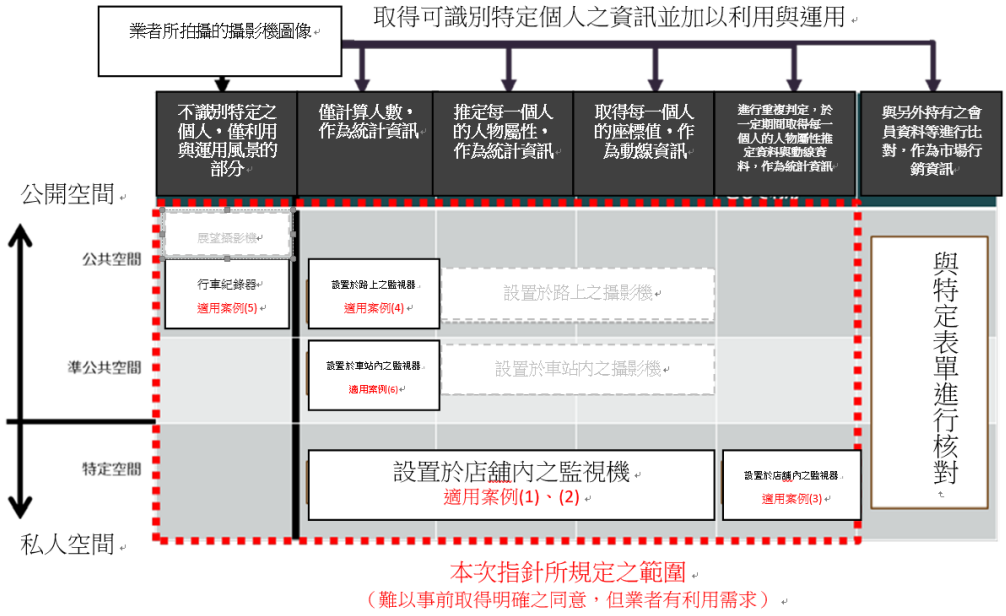


圖 2-10 日本監視器影像加值運用指引規定範圍

資料來源：カメラ画像利活用ガイドブック ver2.0

在說明監視器影像運用方式和拍攝場所等事項後，本指引在檢討具體個案前，先根據日本個資法及影像利用流程，整理合法蒐集、處理及保存監視器影像之方法。

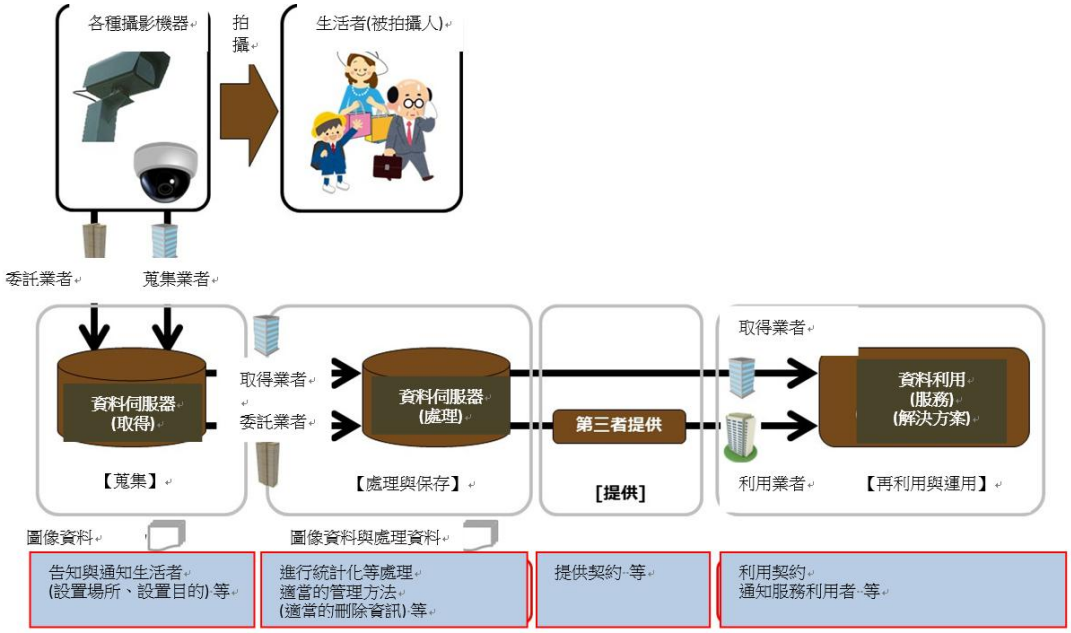


圖 2-11 監視器影像利用流程

資料來源：カメラ画像利活用ガイドブック ver2.0

除根據個資法規定說明如何合法蒐集、處理、保存個資外，工作小組亦進一步整理利用攝影機影像之注意事項。雖然以下注意事項並非法律所規範應採取之措施，但工作小組仍期待業者可以參考注意事項，發展出業界之利用規範。

(1) 基本原則[61]：

監視器影像如為個人資料，除遵守個資法規定外，亦應採取以下措施：

- 規定蒐集、處理、保存、利用等各階段之資料生命週期，並針對伺服器進行風險分析
- 蒐集及利用資料應明確規範利用主體，並設置單一聯絡窗口
- 除設置窗口受理諮詢外，亦應對員工進行訓練，使其能對民眾進行說明
- 針對監視器之利用，應與民眾進行適當溝通，盡量取得民眾認同，並持續蒐集民眾意見，檢討改進方式
- 監視器設置於公共空間時，應遵守場所相關規範

(2) 事前告知與取得資料時之注意事項[62]：

61 IoT 推進コンソーシアム、総務省、経済産業省，《カメラ画像利活用ガイドブック ver2.0》，頁 19-20（2018）。

應預留充分期間進行事前告知，並透過於拍攝場域張貼公告或於官網上聲明等方式，告知民眾拍攝相關事宜。公告內容原則上應包括以下內容：

- 影像內容及利用目的
- 利用主體之名稱及聯絡方式
- 透過利用監視器影響可帶來的便益
- 監視器設置位置及拍攝範圍
- 從監視器影響所生成或抽出資料之概要
- 是否可從生成或抽出資料特定出個人
- 是否會將生成或抽出資料提供給第三人，以及如有提供時應列出提供對象
- 開始利用資料之時期

(3) 處理資料之注意事項[63]：

從監視器影像生成或抽出所需資料後，應儘速刪除原本的影像。此外，關於所生成的資料，如可特定出個人，則應於達成利用目的後儘速刪除。此外，事前應明確說明影像處理方法，並且針對處理後之資料會再特定出個人之風險，進行事前分析。最後，於保存處理後資料時，必須進行加工，避免加工後資料可以特定出個人。

(4) 管理資料之注意事項[64]：

應根據監視器狀況及利用上風險，採取適當的安全管理對策以及資安對策。此外，為防止資訊外洩或目的外利用情況發生，針對所取得之影像資料，以及從該影像所生成或抽出之資料，應規定取得項目、利用範圍、存取權限以及保存期間等。最後，向第三人提供從監視器影像所生成或抽出資料（非個人資料）時，應與該第三人間締結資料利用權限等契約。

最後，本指引以表 2-3 所列 6 個案例為範例，透過情境說明監視器影像所涉及之個資，以及應考量之注意事項。以下為案例 1（設置在店舖內之監視器影像利用）之利用流程和建議注意事項。

62 同前註，頁 21。
63 同前註，頁 23。
64 同前註，頁 24。

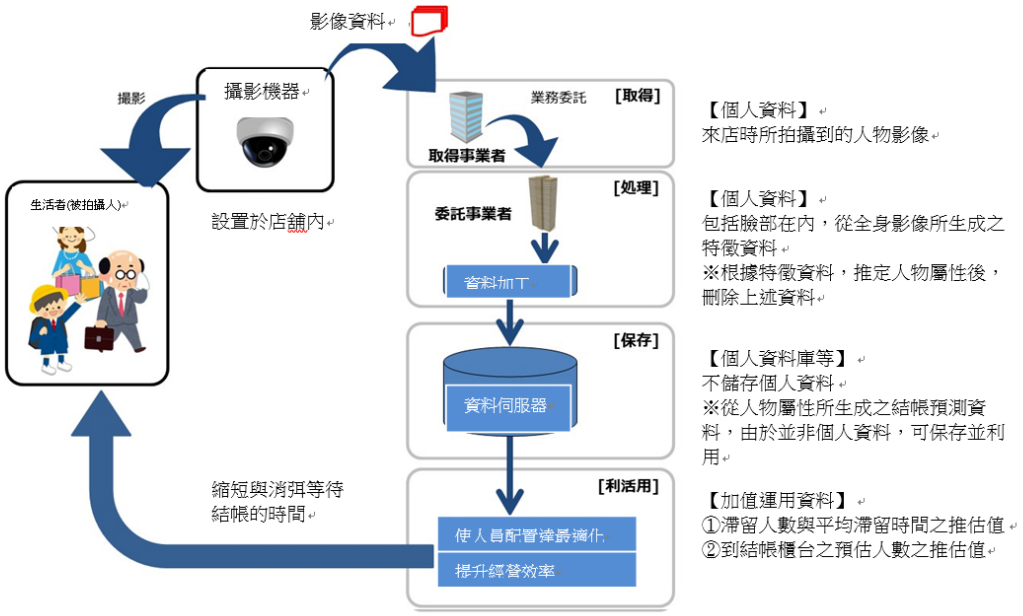


圖 2-12 設置在店內之監視器運用情境

資料來源：カメラ画像利活用ガイドブック ver2.0

表 2-5 根據注意事項之建議採取措施

分類	注意事項	採取措施
基本原則	檢討資料生命週期和設置單一窗口	● 根據資料生命週期，規定系統管理人及建構資料利用體制 ● 設置聯絡窗口
事前告知時之注意事項	進行事前告知	● 於官網上發布訊息 ● 刊登在報紙等媒體
	事前告知內容	● 載明適用範圍，如「以本公司店舖為對象」 ● 載明目的為用於「推估顧客來店以及擁擠狀況」 ● 說明業者利用資料的方式（用於推估預定會產生擁擠狀況之時間等），以及對於民眾帶來的便益（可以縮短結帳等待時間等） ● 不會特定個人 ● 連絡方式
	多國語言對應	● 以不同語言在官網上發布消息
蒐集時之注意事項	通知	● 在店舖入口明顯位置處張貼海報 ● 刊登於官網
	通知內容	● 載明蒐集主體，如「○○股份有限公司」 ● 載明蒐集目的

		● 說明業者利用資料的方式（用於推估預定會產生擁擠狀況之時間等），以及對於民眾帶來的便益（可以縮短結帳等待時間等） ● 不會特定個人 ● 連絡方式
	多國語言對應	● 以不同語言在官網上發布消息
處理時之注意事項	刪除影像	● 不會在系統中處理或保存影像，會刪除影像資料
	處理方法	● 個人資料會處理成無法識別特定個人之資料
	保存資料	● 從人物屬性生成之預估值，會以統計資料形式加以保存
管理時之注意事項	適當之安全管理對策	● 分析影像資料後會立即刪除
	利用範圍與權限	● 利用範圍僅限於公司內部 ● 只有管理員有存取權限
	請求提供時之應對措施	-
	請求刪除時之應對措施	-
	提供給第三人時	● 載明不會提供給第三人
	契約變更之事前告知	-

資料來源：カメラ画像利活用ガイドブック ver2.0

此外，針對上開指引內提到之事前告知和通知方式，為使民眾更容易理解如何進行，總務省和經產省又於 2019 年 5 月制定公布「監視器加值運用指引之事前告知和通知參考案例集」（カメラ画像利活用ガイドブック事前告知・通知に関する参考事例集），進一步說明該如何若實指引要求。

圖 2-13 案例集內容示意

資料來源：カメラ画像利活用ガイドブック事前告知・通知に関する参考事例集

(四) 英國個人資料保護相關指引

1. 監視攝影機實務操作規範

英國資訊專員辦公室（Information Commissioner's Office, ICO）最早在 2000 年時便根據《資料保護法 1998》(the Data Protection Act 1998, PDA）制定中央監視器之使用規範，惟伴隨監視器類型和利用方式增加，上開規範首度在 2008 年時進行更新，以因應數位化和技術進展[65]。

近年來，監視攝影機不再只是單純用於被動紀錄影像，可以主動識別影像進行分析以輔助決策，引起大眾的關注。2012 年《保護自由法》(the Protection of Freedoms Act, POFA)，要求強化對中央監視器或車牌識別、可隨身攜帶之小型監視器、車載監視器、無

65 Information Commissioner's Office[ICO], *In the picture: A data protection code of practice for surveillance cameras and personal information*, p.3(2017).

人機之監視攝影機等……其他監視攝影機之監管，以及設置監視攝影機專員（The Surveillance Camera Commissioner）來確保公共區域之監視攝影機使用上安全[66]。有鑑於此，ICO 於 2013 年 6 月根據 POFA 規定，檢討制定「監視器實務操作規範」（Surveillance Camera Code of Practice），為英格蘭和威爾士政府使用監視器提供指引，並鼓勵民間業者參考上述規範[67]。「監視器實務操作規範」希望能達到個人和社區相信設置監視器可以保護他們，而非監視他們之目的，為此在規範內提出 12 項原則，提供設置監視器之人檢視設置行為是否符合「監視器實務操作規範」[68]：

(1) 監視攝影裝置之使用應限於特定目的，且該目的係為滿足合法目標並具有急迫性。
(2) 使用監視攝影裝置必須考慮對個人和隱私的影響，並需定期檢查以確保合理使用。
(3) 監視攝影系統必須盡可能公開透明，如設置公開窗口以接受民眾回饋或投訴。
(4) 針對所有監視攝影裝置之活動，包括蒐集、保存和使用影像等，必須承擔明確責任。
(5) 使用監視攝影裝置應有明確的規則、政策和程序，並確實將上開規則和程序傳達給應知悉之人。
(6) 監視攝影裝置儲存之影像和訊息數量不得超過裝置本身用途和目的，且目的消失後應予以刪除。
(7) 應限制存取監視攝影裝置儲存之影像和訊息，並明確規範存取權限和方式。
(8) 監視攝影裝置之操作人員，應考慮所有相關技術或操作標準，並盡力符合上開標準。
(9) 監視攝影裝置之影像和訊息應受到適當之安全防護，以防止未經授權之存取和使用。
(10) 應建立有效之審查機制，以確保實務可以落實法遵要求，並應定期公布報告。
(11) 當出於合理目的或迫切需求使用監視攝影裝置時，應以最有效方式使用上開裝置，以協助維護公共安全和執法需求。
(12) 任何用於支援監視攝影裝置之訊息，均應確保其正確性。

2. 落實監視攝影機實務操作規指引

---

66 A National Surveillance Camera Strategy for England and Wales Executive Summary, Gov. UK, https://www.gov.uk/government/publications/national-surveillance-camera-strategy-for-england-and-wales (last visited Oct. 7. 2020),

67 Information Commissioner's Office[ICO], *Surveillance Camera Code of PracticeJune*, p.4(2013).

68 *id*, p.10-11.

為協助民眾確認導入監視攝影裝置符合上開 12 原則要求，ICO 進一步提出「落實 12 項原則之指引」（Code of practice: A guide to the 12 principles）文件，提出 12 項問題讓民眾進行確認[69]：

(1) 監視攝影裝置之目的及用途是什麼？
(2) 是否有進行隱私影響評估？
(3) 是否有設置公開告示說明監視狀況，或有公開管道可以讓民眾聯繫或投訴？
(4) 誰負責監視攝影系統？操作者是否有意識到自己的責任？
(5) 是否有制定明確的規範和程序？操作者是否知道上開規範和程序？
(6) 影像和訊息保存多久時間？如何確保已經刪除影像和訊息？
(7) 是否制定有關存取權限之規定？
(8) 是否有遵守任何操作或技術標準？
(9) 是否確保系統可以安全地取得影像，以及只有經授權之人員才可以存取影像？
(10) 是否定期評估設置監視攝影系統之必要性？
(11) 檢調機關是否可以使用監視攝影裝置生成之影像和訊息？是否制定有關資料儲存、安全和刪除之規定？
(12) 是否使用任何專業技術，如臉部辨識？是否有制定相關政策以確保資料的正確性？

69 Information Commissioner's Office[ICO], *Code of practice: A guide to the 12 principles*, p.2-3(2013).

第三章 智慧建築安全監控法制問答集草案

從國際法制趨勢觀之，可發現世界各國越來越重視個資保護，強調個人對自身資料的控制權，GDPR 甚至強調在設計階段就要納入隱私概念。然而，強調個資和隱私保護之立法趨勢，某種程度上與物聯網發展相互衝突，透過感測器蒐集資料進行分析、處理和利用之過程，改變傳統蒐集資料的方式，使蒐集資料的人難以當面取得當事人同意，而部份原本並非個人資料之資料，在與其他資料比對後，亦有可能成為個人資料，使整個情況變得更加複雜。有鑑於此，為協助有蒐集、處理、利用個資需求者，在遵守相關規範前提下使用個人資料，國際上往往透過制定指引或問答集等方式，來說明該如何落實法規要求。

雖然目前國際間並無以智慧建築為對象之指引，惟伴隨物聯網快速發展，監視器原先拍攝之影像資料，其蒐集、處理、利用方式逐漸成為輿論關注焦點，故歐盟、英國和日本均有特別針對監視器制定指引加以規範。鑑於我國在智慧建築標章和設計技術規範中，資訊通信及安全防災都是必備項目之一，加上《建築技術規則》針對建築物安全維護技術有特別加以規範，故歐盟、英國和日本有關監視器之個資指引和案例集，應可作為本研究編寫問答集之參考。

在指引內容及編排方式上，歐盟「監視器影像個人資料處理指引 3/2019」主要在說明監視器影像資料之利用，該如何遵守 GDPR 規範，並針對處理個人資料之合法性、資料主體權利、個資儲存和刪除等常見問題加以說明，惟因上開指引是以文字進行說明，沒有輔以任何圖示或案例，對一般民眾而言，可能會比較難以理解，閱讀上較為吃力；英國自 2000 年就開始針對中央監視器進行規範，並於 2012 年透過《保護自由法》要求設置監視攝影機專員，用於確保監視攝影機之運作，而 ICO 亦於 2013 年制定相關規範和指引，協助業者於導入上開設備時符合法規要求。英國有關監視攝影機之設置與使用，從法律、指引到各項技術標準等，有十分全面且詳細的規範，惟上述規定仍係以文字為主，可能還是會有難以理解及遵守的問題。英國 ICO 或許亦是注意到上述問題，故於後續公步「落實監視攝影機實務操作規指引」，提出 12 個問題，讓業者可以自評是否有遵守法規。

與上述以文字為主的指引或規範不同，日本「監視器影像加值運用指引第 2 版」，其先根據影像資料之生命週期，提出各階段處理個人資料時之注意事項，再依照影像資料之利用方法和拍攝範圍，描繪出 6 種具體案例，最後針對上述案例，以情境方式，說明該如何落實前面所提出之注意事項。由於透過具體案例說明該如何落實個資法要求之方式，對於不熟悉個資法的一般民眾而言，較能迅速了解並將其運用在實際個案中，故本計畫之問答集，在編排方式上擬參考日本作法，透過具體案例進行說明。

本計畫在期中報告時參酌「監視器影像加值運用指引第 2 版」以案例說明之作法、歐盟「IT 治理與 IT 管理之個人資料保護指引」將資料生命週期分為五大階段，針對不同階段依序說明各項問題之方式，以及日本「網路安全相關法令 Q&A 手冊」之編排架構，認為在問題後列出參考法條及判例有助於讀者深入閱讀，故規劃問答集草案架構如下圖：

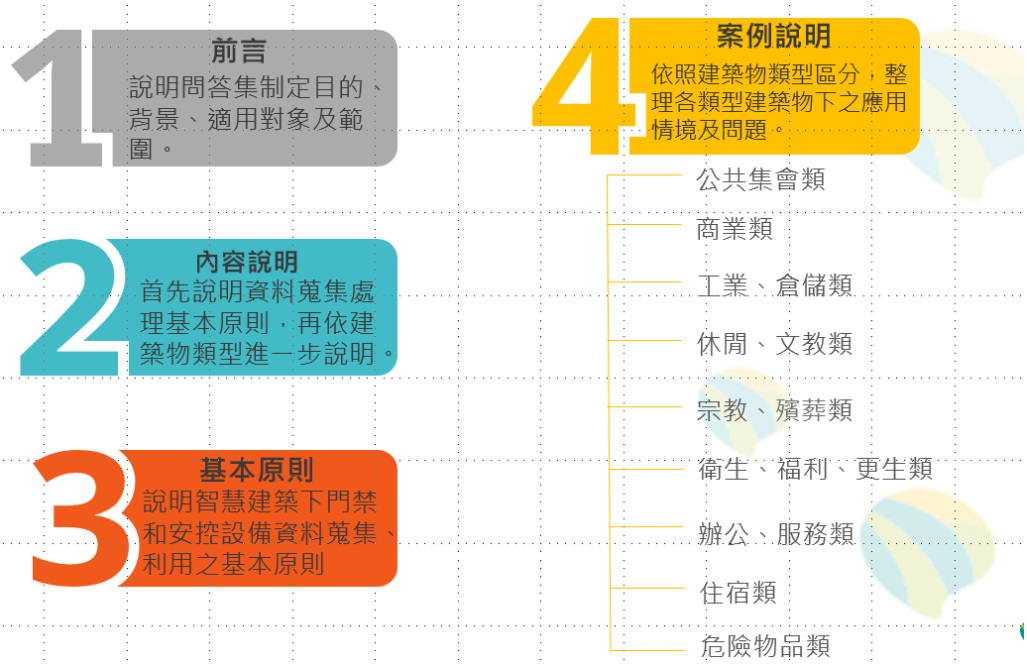


圖 3-1 問答集草案架構（期中）

資料來源：研究團隊自行繪製

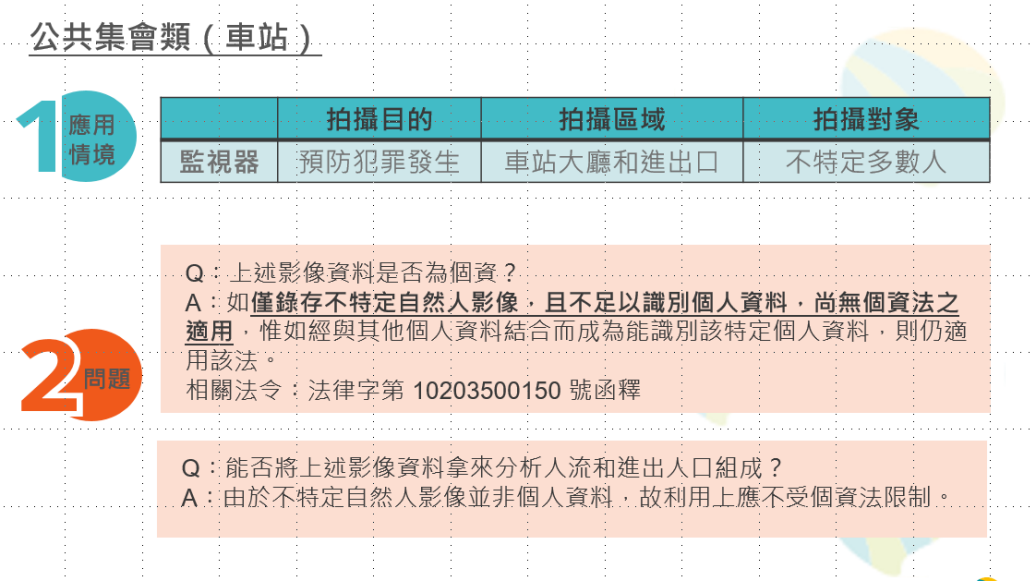


圖 3-2 應用情境和相關問題示意圖（期中）

資料來源：研究團隊自行繪製

本計畫於 2020 年 7 月 9 日舉行座談會（附錄十），就上述問答集架構徵集專家意見，與會專家建議重點如下：

1. 安全監控設備範圍很廣，建議標題可標明為「人員」監控；另「監控」

二字可能使民眾產生疑慮，鑑於問答集面向使用者，應優先考慮排除使用者疑慮，建議從蒐集資料目的在於管理和提供服務出發，思考如何調整用語，並在問答集內強調智慧建築蒐集、應用資料之目的。

2. 關於個資利用之特定目的，可以從建築安全營運管理和服務行為出發，再進一步因應建築物類型、需求，以及所有權人等細化。在資料管理上，必須強調原始資料不能被竄改，且從第一線人員到管理階層，都需要透過法令加以規範（如需取得認證），以確保資料安全。
3. 關於監視設備，未來或可考慮在《建築技術規則》內增加其他空間，以及設置位置等規定。惟智慧建築蒐集資料之目的，在於提供或優化各項服務，故應先考慮從《公寓大廈管理條例》著手，加強管理層面之規範，並因應建築物類型區分不同使用目的。
4. 建築物種類眾多，建議今年先完成通案性原則，並釐清優先順序，如供公眾使用之建築物較常導入安全監控設備，先針對該類型建築物蒐集相關問題。
5. 伴隨技術進步，建築物內管制措施也需要與時俱進，除國內廠商外，建議可了解跨國大廠作法。

參酌上述建議，本計畫重新調整問答集架構和內容，先後於 2020 年 8 月 20 日（附錄十三）、9 月 14 日（附錄十四）和 9 月 17 日（附錄十五）提供三個版本之問答集草案，最終於 9 月 26 日工作會議（附錄九）確認問答集架構和格式，在內容方面，則保留前言和使用說明等文字，刪除有關定義、用語說明和個資法相關之 QA，全部改為以案例為主，透過情境說明具體個案中可能涉及哪些法律問題及建議作法。

本計畫根據上述研究、座談會專家意見，以及工作會議結論，重新修正並研提「智慧建築資料應用法制課題及因應對策問答集」草案。

第四章 結論與建議

第一節、 結論

本研究依據規劃時程，已完成相關業者訪談，了解國內門禁系統及安全監控設備狀況和個人資料蒐集、處理、利用現況，分析智慧建築安全監控設備資料應用法制障礙，並蒐集國內外相關文獻，整理歐盟、英國和日本有關安全監控設備或個資保護之法制和具體措施。

綜整我國門禁系統及安全監控設備運用狀況及推動資料應用之法制障礙，參酌國外有關監視攝影裝置影像資料及其他與個資和隱私保護相關之指引後，本研究於期中提出問答集草案架構規劃，並舉辦座談會（附錄十），就問答集內容和編排方式等徵集相關意見。鑑於座談會上與會專家，以及期中審查之審查委員（附錄十二）均建議應調整問答集適用對象和分類方式，故本計畫依照上述意見進行修正，並陸續提出三種版本之問答集草案，最後於工作會議（附錄九）上確認問答集格式，以及內容需保留前言和使用說明等文字，刪除有關定義、用語說明和個資法相關之 QA，全部改為以案例為主，透過情境說明具體個案中可能涉及哪些法律問題及建議作法。

本計畫依據上開研究結果、專家意見和會議結論，於期末提出「智慧建築資料應用法制障礙及因應對策」問答集草案，並參酌期末審查意見（附錄十三）進行修正，提交成果報告及修正後問答集草案。

第二節、 建議

針對本計畫所進行之研究與分析，研提立即可行建議及長期建議如下：

建議一

檢討制定智慧建築資安相關指引：立即可行建議

主辦機關：內政部建築研究所

協辦機關：資訊工業策進會

本計畫今年度研提我國「智慧建築資料應用服務法制課題及因應對策問答集」草案，以門禁和安全監控系統之應用情境為例，針對具體個案中可能發生之法律問題加以說明，期能降低一般使用者對於蒐集個人資料後利用人工智慧等技術加以分析，進提供各項智慧化服務之疑慮。在釐清門禁和安全監控系統在法律適用上之疑義後，由於在物聯網時代，建築物內所導入之各項資通訊應用，可能因作業系統、應用程式或設備本身存在漏洞，洩漏所蒐集和儲存之資料，或導致相關系統和設備無法正常運作，產生安全防護上之隱憂。有鑑於此，建議內政部建築研究所應就建築物導入資通訊應用之注意事項提出指引，健全智慧化居住空間環境。

建議二

檢討增修公寓大廈規約範本：長期建議

主辦機關：營建署

協辦機關：內政部建築研究所

建築物資料之利用，必須由資料所有權人和利用者之間約定利用方式、期間和範圍。以我國公寓大廈為例，公寓大廈管理委員會為處理社區內行政事務，可能有調閱、公布或向他人提供門禁資料和監視器影像資料之需求，如管理委員會能事先與住戶透過公寓大廈規約加以約定，可以避免未來產生糾紛，故建議日後可考慮檢討修正公寓大廈規約範本，加入建築物資料蒐集、處理和利用等事項，以促進智慧建築資料利用。

附錄一：中興保全訪談紀錄

一、 中興保全練文旭協理訪談紀錄

（一） 會議資訊

會議時間：108 年 03 月 5 日 10：00 至 11：00

會議地點：中興保全內湖分公司

受訪談人：練文旭協理

訪談人：王自雄、周晨蕙（職稱略）

記　錄：周晨蕙

訪談題目：智慧門禁及安全監控設備資料應用現況及法制問題

（二） 訪談提綱

1. 關於智慧門禁及安全監控系統，從開發到實際投入使用，可能會涉及哪些產業？其中哪些單位才會實際蒐集、處理及利用到個人資料（如安控產業僅將門禁及監控系統賣給保全服務消費者，故不會接觸到個人資料）？上述設備所蒐集到的資料，是否有約定所有權歸屬？
2. 在 AI 等新技術發展下，產品研發過程中可能需要利用個人資料（如將資料用於機器學習），則在資料所有權可能屬於場域（如社區、大樓管委會等）的狀況下，系統廠商該如何取得資料進行研發？此外，由於安控設備蒐集資料的目的在於管理場所進出安全，將個資用於研發可能違反個資法規定，目前實務如何因應上述問題？
3. 承上，縱使場域同意提供資料給系統廠商利用，惟安控設備蒐集資料的目的在於管理場所進出安全，並非進行產品研發，故此種行為有可能違反個資法規定。針對上述狀況，目前實務上是否有考慮採取一些作法？如請場域告知被蒐集個資之當事人，蒐集的資料將用於產品研發等。
4. 伴隨時代發展及觀念轉變，許多資料（如熱感應影像、車牌、個人行動軌跡等）在結合其他資料後，都有可能被認為是個人資料，加上民眾越來越注重個資和隱私保護，對於人臉辨識等技術感到

不安，這些狀況是否成為安控產業研發和推廣新產品的障礙？

5. 針對智慧門禁系統和安全監控設備可能涉及之個資法相關規定，擬請教以下問題：

(1) 根據個資法規定，除符合例外情形外，在蒐集個人資料前應告知當事人，針對實務目前告知當事人之方式及內容，請教以下問題：

i. 門禁系統或安全監控設備依其特性，可能無法逐一告知當事人，針對上述狀況，除張貼佈告外，目前實務可能還會採取哪些作法？

ii. 告知當事人時，應清楚告知蒐集目的、個資類別、資料利用期間、利用方式及利用範圍等，惟伴隨資訊科技發展，想要在事前清楚說明越來越困難。請問實務上是否曾發生因事前未清楚告知（如僅告知有監視器，但沒有說監視器蒐集影像的利用目的和範圍），導致使用者後續提出抗議等狀況？

iii. 關於告知當事人之規定，如果符合個資法第 8 條第 2 項所列 6 種例外情形，業者可以不用告知當事人。以實務觀點來看，目前所列 6 種例外情形是否已足夠應付實務需求？

iv. 目前實務上可能會採取哪些作法（如導入第三方驗證），以確保上述告知行為符合個資法要求？

v. 承上，本計畫擬針對上述狀況編寫問答集提供業者參考，以利業者落實個資法遵需求。針對問答集內容及編寫方式，請教國霖機電意見。

(2) 根據個資法規定，蒐集處理個人資料應符合特定情形和特定目的，針對實務目前蒐集處理個人資料的狀況，請教以下問題：

i. 目前個資法有關蒐集處理個資之限制，從實務觀點來看，是否過度限制業者對個資之蒐集與處理？

ii. 根據現行法規定，如門禁系統或安全監控設備蒐集無法符合個資法第 19 條有關特定情形之要求，則業者想要蒐集處理個資，就只能取得當事人同意。目前實務上主要係以何種方式取得當事人同意？

iii. 假使門禁系統或安全監控設備所蒐集的資料逾越必要範圍，如要求社區訪客出示證件換取門禁卡即可達到管理目的時，還要求訪客拍照並提供姓

名、身分證字號、電話等個人資料，縱使業者已經取得當事人同意，上述行為仍然違反個資法規定。由於不同門禁系統和安全監控設備所蒐集的資料類型不同，門禁卡可能只要出示證件就可以換取，但生物辨識系統需要蒐集當事人指紋，目前實務係如何根據不同系統設定蒐集資料類型，以及確保蒐集處理行為符合個資法要求？

iv. 承上，本計畫擬針對上述狀況編寫問答集提供業者參考，以利業者落實個資法遵需求。針對問答集內容及編寫方式，請教國霖機電意見。

(3) 根據個資法規定，除符合特定情形外，個人資料之利用應於特定目的範圍內為之，如門禁系統蒐集個資之目的是管理場所進出安全，則其蒐集到的個資就只能用於場所進出管理，不能用於產品研發。針對實務目前利用個人資料的狀況，請教以下問題：

i. 目前個資法有關利用個人資料之限制，從實務觀點來看，是否過度限制業者對個資之利用？

ii. 針對個人資料之利用，目前實務上可能會採取哪些作法（如導入第三方驗證），以確保利用行為符合個資法要求？

iii. 本計畫擬針對上述狀況編寫問答集提供業者參考，以利業者落實個資法遵需求。針對問答集內容及編寫方式，請教國霖機電意見。

(4) 根據個資法規定，當事人可以通知請求業者刪除、停止處理或利用其個人資料，如業者（如物業）依照上開規定刪除當事人個資，是否有可能影響門禁系統或安全監控設備之運作？

(5) 根據個資法規定，業者應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏，警政署亦制定「保全業個人資料檔案安全維護管理辦法」，以規範保全業落實個資法要求。惟在網路和雲端服務技術的發展下，資料外洩和被竊取的可能性越來越高，未來該如何妥善保護個人資料？

6. 我國擬於 2020 年修正個資法，為在個資保護和科技發展間取得平衡，針對未來修法方向，請教國霖機電意見，作為科法所後續研提建議之參考。

（三） 會議記錄

1. 王自雄主任首先說明拜訪目的，為執行「智慧建築安全監控資料應用法制課題及對策之研究計畫」，擬深入了解智慧門禁系統和安全監控設備者個人資料蒐集、處理、利用狀況及困難，對應我國個資法上相關規定及司法實務，找出推動智慧建築資料應用之法制障礙，並針對具體個案編寫問答集，引導及協助業者落實我國個資法遵需求。本次訪談希望能了解國內智慧門禁系統和安全監控設備個人資料運用狀況，以及實務工作所面臨的問題，作為後續研提法規建議和編寫問答集之參考。
2. 練文旭協理：中興保全係協助客戶建立保全系統，不會直接接觸到個人，蒐集處理及維護個人資料者均為客戶，中興保全頂多協助客戶代為保管資料。目前安全監控設備已經廣泛運用影像辨識技術，如車牌辨識、人臉辨識等，惟影像辨識技術需要使用大量資料來訓練 AI，故對中興保全而言，目前最大的問題是能否利用上述代管資料進行研發。
3. 練文旭協理繼續說明：以中興保全目前的營運模式為例，我們將監視器賣給 A 公司後，A 公司可能會與中興保全另外簽約契約，將資料交給中興保全代管，此時資料雖然儲存在中興保全，但實際上蒐集處理個資的仍是 A 公司，資料所有權人也是 A 公司。假使中興保全想要利用上述資料進行研發，可能會面臨以下問題。首先，我們不清楚上述資料是否為個人資料，如單純的臉部影像，以及公共區域影像等。其次，為利用臉部影像等個人資料，歐洲有些廠商會透過只儲存臉部影像的特徵，或將生理特徵轉成參數等方式進行去識別化，但我們不清楚去識別化在國內要作到什麼程度，亦無法保證在去識別化之後，A 公司就會同意將資料提供給中興保全使用。最後，由於這些資料屬於 A 公司所有，則中興保全是只要取得 A 公司的同意就好，還是仍然需要取得被拍攝的當事人同意？由於中興保全不清楚 A 公司和當事人之間的狀況，所以情況變得很複雜。
4. 王自雄主任：根據我國個資法第 2 條規定，練協理剛剛提到的資料，只要能以直接或間接方式識別出該個人的話都是個資，由於許多資料必須經過判斷才能確定是否為個資，故科法所才想藉由本計畫制定指引提供業界參考。另外，關於去識別化標準，經濟部標準檢驗局 CNS 29100 及 CNS 29191 標準以及「個人資料去識別化過程驗證要求及控制措施」等，或可作為業界進行去識別化作業之準則。最後，請教中興保全的客戶在蒐集個資時可能出現的問題，以及不願意提供資料給中興保全的顧慮為何？
5. 練文旭協理：設置安控系統之公司，進出的人員包括員工和訪客等，公司在蒐集個資時，可能都已取得員工的同意，但訪客的部

份卻不一定，縱使有取得同意，也不一定有清楚地告知訪客蒐集資料之目的、範圍和利用方式。另外，由於客戶蒐集個資之目的在於管理場所進出狀況，並非進行產品研發，如果提供給中興保全，可能還會有個資法上目的外利用的問題。基於上述原因，中興保全目前都是自己拍攝技術研發所需之影像。

6. 周晨蕙研究員：關於蒐集訪客個資的問題，法務部法律字第10603505040號函指出，就算取得訪客同意，蒐集處理訪客個人資料仍應符合比例原則，目前實務上往往會蒐集訪客姓名、證件、電話等資料，甚至將證件拍照建檔，可能已經逾越特定目的之必要範圍。然而，雖然法務部已經做出上述函釋，但想要釐清資料蒐集是否逾越必要範圍並不容易，故訪客個資之蒐集容易成為灰色地帶。
7. 王自雄主任：關於前面提到的去識別化標準，請問練協理目前業界有建立自己的標準或規範嗎？
8. 練協理：目前業界的共識，只有個資經去識別化後可以使用而已。關於去識別化標準，如果政府能帶頭制定規範，民間就會自發跟進，如IP Camera，經濟部公告「影像監控系統資安標準」後，又與NCC聯手訂定IP CAM認證制度，故業界亦積極參與輔導，配合政府要求。雖然目前已經有去識別化的標準或認證制度，但由於這樣做會增加營運成本，所以如果政府或客戶沒有要求，一般公司恐怕不會考慮導入相關標準或認證制度。
9. 王自雄主任：關於影像辨識技術，未來可能有哪些運用模式？曾有哪些相關應用因為受限於法規，無法有進一步發展。
10. 練文旭協理：就我所知，國外計程車監控影像會以加密方式處理，只有警方調閱時才能解密觀看，國內還沒有採用這麼細膩的管理方式。另外，中興保全曾經拜訪警政署，了解門禁系統連線比對贓車車牌或通緝犯等公開資料之可行性，假使可以連線比對，則在贓車或通緝犯進入特定場域時，就可以即時通知警政單位處理。然而，由於上述作法會有個資和人權上的疑慮，故警政署的立場仍偏向保守。
11. 練文旭協理繼續分享實務狀況：超商、賣場或銀樓容易遇到奧客、慣竊或搶匪，故有建立黑名單系統的需求，在奧客或慣竊等黑名單進入場域時就加以注意。然而，由於黑名單資料涉及個資，不能與同業共享，故保全公司目前只能幫各場域建立自己黑名單系統，無法進一步達到聯防的效果。
12. 周晨蕙研究員：最後請教練協理，目前業界在販售安控系統給客戶時，是否會特別告知客戶相關注意事項，如個資蒐集處理利用之方式等？

13. 練文旭協理： 除非未來政府要求保全業者必須告知客戶，否則業界不會特別提醒客戶。
14. 王自雄主任：謝謝練協理寶貴的經驗分享。針對特定資料是否為個資、告知方式，以及訪客個資蒐集、去識別化程度等灰色地帶問題，本計畫未來將進一步研析，並透過問答集或指引方式加以澄清，提供業者參考。

附錄二：台灣智慧建築協會訪談紀錄

（一） 會議資訊

會議時間：108 年 03 月 23 日 10：00 至 11：00

會議地點：台灣智慧建築協會

受訪談人：溫琇玲名譽理事長

訪談人：王自雄、周晨蕙（職稱略）

記　錄：周晨蕙

訪談題目：智慧建築資料類型及運用狀況

（二） 訪談提綱

1. AIoT 發展為我國安全監控產業帶來許多應用機會與挑戰，安控設備可應用於智慧建築、智慧家庭、智慧工廠等不同領域，請教目前安控設備在建築物內的運用情境，以及在過程中可能蒐集的資料類型。此外，針對上述設備所蒐集的資料，未來可能衍生出哪些應用和服務？
2. 當安控產業協助在特定場域內布建門禁系統等設備後，實際接觸並蒐集處理個人資料者應為建築物管理者、管理機關、所有權人、使用人、管理委員會等，請教目前場域蒐集、處理、利用個人資料的狀況。

    (1) 關於智慧門禁及安全監控系統，其資料蒐集處理利用的過程可能涉及哪些關係人？
    (2) 目前安控設備所蒐集之資料，原則上應屬於場域所有，第三方想要利用智慧建築所蒐集之資料，可能的障礙有哪些？如資料所有權歸屬過於複雜，或不確定是否有告知並取得當事人同意，故不敢將個資提供給他人等。
    (3) 根據個資法規定，蒐集、處理、利用個人資料原則上應告知並取得當事人同意，並注意不得逾越必要範圍。目前布建於建築物內部之安全監控設備，如欲蒐集處理利用個人資料，通常會採取哪些措施（如張貼告示），

以告知並取得當事人同意？

(4) 承上，如果場域沒有採取任何措施，其最大的困難是什麼？例如不清楚個資法規定，或因為建築物內往來人員複雜，根本無法告知並取得當事人同意等。

(5) 智慧建築所蒐集到之個人資料，縱使已經取得當事人同意，惟因安控設備蒐集資料之目的在於管理場所進出安全，根據個資法規定，仍然無法將上開資料用於研發或分析。想要解決上述問題，可以將個資去識別化、假名化或匿名化，惟對於想要利用個資的第三方而言，進行上述處理會額外增加成本，且部份資料去識別化後無法利用（如臉部辨識資料），請教溫老師對於上述狀況的意見。

(6) 承上，經濟部標準檢驗局制定 CNS 29100 及 CNS 29191 標準，以及「個人資料去識別化過程驗證要求及控制措施」，作為個資去識別化依據。惟對於一般民眾而言，即便有上開標準和措施，仍然無法判斷個資是否已經去識別化。從制度上來看，如能建立第三方認證機制，由第三方協助確認個資是否已經去識別化，或由特定機構將個資去識別化後提供第三方利用，是否更能有效促進資料之利用？

(7) 針對特定資料是否為個資、個資蒐集處理利用之原則和例外規定，以及個資去識別化等問題，本計畫擬透過問答集方式加以說明，針對問答集內容及呈現方式，請教溫老師意見。

3. 我國擬於 2020 年修正個資法，為在個資保護和科技發展間取得平衡，針對未來修法方向，請教溫老師意見，作為科法所後續研提建議之參考。

（三） 訪談紀錄

1. 王自雄主任首先說明拜訪目的，為執行「智慧建築安全監控資料應用法制課題及對策之研究計畫」，擬深入了解智慧門禁系統和安全監控設備者個人資料蒐集、處理、利用狀況及困難，對應我國個資法上相關規定及司法實務，找出推動智慧建築資料應用之法制障礙，並針對具體個案編寫問答集，引導及協助業者落實我國個資法遵需求。本次訪談希望能了解國內智慧門禁系統和安全監控設備個人資料蒐集和利用之狀況，作為後續研提法規建議和編寫問答集之參考。

2. 周晨蕙研究員：研究團隊之前曾拜訪中興保全等安控業者，由於安控產業僅協助場域布建相關設備，不清場域蒐集處理利用個資的狀況，故想請教理事長目前智慧建築內安控設備之運用情境及所蒐集之資料類型等細節。另外，業者也表示曾想取得場域所持有之資料進研發，惟因場域對此抱有疑慮，故最終無法取得相關資料。針對上述狀況，想請教老師可能的問題出在哪裡？
3. 溫琇玲理事長：在談論智慧建築資料相關問題前，必須先釐清一些概念。首先，智慧建築是指應用網路、監測設備及系統整合等技術，具有自動感知、分析及回應等功能之建築物，根據公寓大廈管理條例第 3 條，建築物內部空間可區分為專有部份、共用部份、約定專用部份和約定共用部份，由於專有部份屬於私人空間，是否布建智慧化設備端視個人而定，故智慧建築實際上只談共用部份，不管專用部份。以我國智慧建築標章為例，標章內所有評估項目都是針對公共空間之佈線、資訊通信、系統整合和設施管理，唯一與專用部份有關的只有健康舒適指標下 7.1「室內空間健康舒適」評估項目，該項目評估內容包括室內溫度、濕度和二氧化碳偵測及資訊顯示，與個資有關者為 7.2.1「具傳輸功能之生理監測裝置（如血壓偵測、心跳偵測、血糖偵測等）」。然而，7.2.1 之評分重點在於建築物內部是否有設置相關感測裝置，以及該裝置之傳輸功能（發生狀況時能通知外界），與是否蒐集個人資料無關。
4. 溫琇玲理事長繼續說明共用部份之資料歸屬及取得等問題：由於智慧建築聚焦於公共空間，故所產生的資料基本上都是公共空間的資料。由於在公共空間布建安控設備及取得相關資料都是為了照顧住戶的權益，根據公寓大廈管理條例第 36 條，管理上開設備及資料屬於管理委員會職務之一，故如有需要取得相關資料，目前都會詢問管委會。我聽說有些管委會會對外出售上開資料，並將販售所得回饋住戶，由於有回饋，故住戶通常都不會表示反對；另外，我也聽過有些管委會是無償提供資料給他人。無論是有償或無償授權，上開資料如涉及個人資料，都需要經去識別化處理。
5. 溫琇玲理事長繼續說明：由上所述，可知相對於專有部份，公共空間的資料並沒有那麼難以取得。針對專有部份，安控設備的應用情境主要是智慧住宅、智慧家電和健康照護等，如監測獨居老人開冰箱或電視的狀況，當沒有開電視或冰箱時便通知大樓管理員和家人探視，以免發生不測。由於上述設備所取得之資料為生理數據或日常行動資料，根據個資法規定均屬於個

人資料，故台灣智慧建築協會曾針對遠雄建設推出之智慧住宅，要求其必須與住戶簽約，惟根據遠雄表示，因相關監控設備費用昂貴，住戶擔心將設備弄壞故未使用，所以最後並沒有簽署同意書。

6. 溫琇玲理事長：現代科技可以輕易取得建築物內的個人資料（如日常行動資料等），即便不知道該資料所指涉的對象是誰，透過資料勾稽，想要找出特定當事人身份亦不困難，空有大量資料而無法利用，才是目前所面臨的最大問題。對於想要利用這些資料的單位來說，他們根本不知道被蒐集資料的對象是誰，這樣真的不能利用嗎？此外，有時候進行分析時需要知道個人的基本資料，去識別化反而會使資料喪失價值。
7. 王自雄主任：國發會預計於今年提出個資法修正草案，因應大數據發展趨勢，未來個資法應鼓勵資料利用，重點應放在如何規範個資之使用，而非限制利用。謝謝溫理事長提智慧建築領域之案例，我們會將上述案例納入問答集，透過情境說明智慧建築相關個資問題。除個資法相關問題外，想進一步請教理事長目前是否存在其他可能影響智慧建築資料應用之障礙。
8. 溫琇玲理事長：關於智慧建築資料運用，台北市政府推動社會住宅雲服務計畫，規劃建置臺北市公宅管理雲，作為公宅基本管理服務使用，並預期透過本計畫與民間業者合作規劃建置公宅生活服務雲，提供多元加值的生活服務功能[70]。上述雲端服務平台立意良善，但存在兩大問題。第一個問題是平台資料都委由物業代管，換物業後資料就會被帶走，無法真正掌握在台北市政府手上。這個問題其實不僅發生在台北市公宅管理雲，而是所有智慧建築都面臨的問題，智慧建築最重要的就是資料，物業只是接受委託代為管理，資料必須由始自終都屬於智慧建築。
9. 王自雄主任：資料治理（data governance）是當前社會重要的公共政策課題之一，如何在智慧建築內落實資料治理，使關係人士均可透過資料揭露獲取利益，應是值得關注的重要課題。此外，由於智慧建築所蒐集之資料可能為個人資料，故該如何將個資法規定落實於資料治理層面，亦須進一步探討。
10. 溫琇玲理事長繼續說明：除資料治理問題外，另外一個平台存在的問題是沒有考慮到市政府、物業和住戶所需要的資料類型不同。物業在公寓大廈內主要工作為設備維護、生活服務和人

---

70 〈智慧城鄉：臺北市智慧社區雲服務計畫〉，Smarttaipei，https://smartcity.taipei/project/123（最後瀏覽日期：2020/03/26）。

事管理等，住戶東西損壞向物業報修，住戶取得服務後，物業向市政府請款，在這件事中市政府需要的是財務資料，物業需要的是通報紀錄，而住戶要的是維修紀錄，三者所需資料類型不同，故比較好的作法應該是建立一個資料庫，三者都可以從中取用資料，只是根據權限所取得的資料類型有所區別。其實目前智慧建築平台已有成功案例，如我國最早取得智慧建築標章之士林電機仰德大樓。

11. 溫琇玲理事長：未來台灣智慧建築協會將協助內政部建築研究所建立中央社會住宅建築數據中心，如一切順利，未來業主除可使用利用該平台資料外，亦可將平台推廣到民間，提供民間業者使用。此外，如能有一個建築數據資料庫，亦能用於比較建築物能耗資訊。
12. 王自雄主任：台灣智慧建築協會去年起執行內政部建築研究所「智慧建築空間性能數據蒐集暨雲端平台應用計畫」，請教目前建置進度。
13. 溫琇玲理事長：目前協會已經完成平台架構，今年將鎖定空調、溫度、照護等維護資料進行蒐集。智慧建築相關資料分為靜態資料和動態資料兩種，前者如圖資、BIM（建築資訊模型），後者為 IoT 設備所取得之資料，如溫度、臉部辨識資料等。動態資料隨時都在更新，依照目前技術，設定多久取得一次動態資料及取得範圍並不困難，但動態資料容易涉及個人資料和隱私，所以仍須取得個人同意，不能僅有管委會的同意。
14. 溫琇玲理事長繼續說明：其實智慧建築資料真正的問題不在於如何取得資料，而是大家根本不知道要哪些資料，所以無法在建造時依照需求布建設備，在沒有資料的狀況下，也不用談後續資料蒐集處理利用等問題。此外，資料治理也是智慧建築非常重要的課題。綜上所述，智慧建築資料應用總共有三大問題：要蒐集哪些資料、個資問題及資料治理。
15. 王自雄主任：資策會科法所感謝溫琇玲理事長寶貴的經驗分享。

附錄三：國霖機電訪談紀錄

（一） 會議資訊

會議時間：108 年 03 月 31 日 14：30 至 15：30

會議地點：國霖機電

受訪談人：徐春福執行長、張凱強經理

訪談人：周晨蕙

記　錄：周晨蕙

訪談題目：智慧建築弱電系統運用狀況及問題

（二） 訪談提綱

1. AIoT 發展為我國安全監控產業帶來許多應用機會與挑戰，安控設備可應用於智慧建築、智慧家庭、智慧工廠等不同領域。針對智慧門禁系統和安全監控設備於智慧建築內蒐集資料的狀況，請教以下問題：

    (1) 智慧門禁系統和安全監控設備之應用情境。
    (2) 智慧門禁系統及安全監控設備蒐集之資料類型，其中是否包含個人資料？
    (3) 智慧門禁及安全監控系統主要會蒐集哪些人的資料？針對訪客或路人，該如何履行個資法上有關告知和取得同意之要求？
    (4) 在蒐集資料的過程中，除個資法限制外，可能還會遭遇哪些困難？如不知道要蒐集哪些資料，故無法確定要安裝哪些設備等。

2. 針對智慧門禁系統和安全監控設備所蒐集資料，後續如何進行保管和處理，請教以下問題：

    (1) 智慧門禁系統和安全監控設備所蒐集到之資料，目前主要是由誰來負責管理？如安裝監控設備之保全業者、物業或建築物管理者（如管委會）。
    (2) 承上，如資料是由保全業者或物業代管，則在更換業

者時，資料會如何處理？

3. 針對資料所有人或第三方想利用智慧門禁系統和安全監控設備所蒐集之資料，請教以下問題：

   (1) 針對智慧門禁系統和安全監控設備所蒐集之資料，請教目前可能有哪些單位想要利用上述資料，以及想要利用的資料類型和應用情境。
   (2) 如果有人想要利用上述資料，目前可能會與哪些單位進行接洽？假使上述單位（如管委會）想要將資料提供給第三方，但這些資料涉及個資，他們可能會以何種方式取得個人同意？

4. 針對智慧門禁系統和安全監控設備所蒐集之資料是否為個資、個資蒐集處理利用之原則和例外，以及個資去識別化等問題，本計畫擬以問答集形式呈現，並透過情境加以描述，使讀者更容易了解。針對上述問答集內容和呈現方式，請教徐執行長意見。

（三） 會議摘要

1. 周晨蕙研究員首先說明拜訪目的，為執行「智慧建築安全監控資料應用法制課題及對策之研究計畫」，擬深入了解智慧門禁系統和安全監控設備者個人資料蒐集、處理、利用狀況及困難，對應我國個資法上相關規定及司法實務，找出推動智慧建築資料應用之法制障礙，並針對具體個案編寫問答集，引導及協助業者落實我國個資法遵需求。本次訪談希望能了解國內智慧門禁系統和安全監控設備，亦即弱電系統個人資料蒐集和利用之狀況，作為後續研提法規建議和編寫問答集之參考。
2. 徐春福執行長：張經理為本公司弱電系統負責人，關於國內社區裝設及使用弱電系統狀況，請張經理說明。
3. 張凱強經理：國內高級社區著重於發展智慧家庭，智慧建築則強調公共區域，而公共區域之監控以設備監控為主，故蒐集的資料大多並非個資。建築內的監控系統分為一般監視器和監控大樓設備運作狀況的監視系統，前者目前主要類型有純影像拍攝、動態偵測和熱感應等，攝影機所取得資料之應用方式要看其結合的軟體而定，如影像拍攝結合人流分析軟體，並將分析結果用於行銷；後者主要是用於大樓管理和維護，目前大樓內所謂的監控系統，主要是指這種設備監控系統。針對門禁系統，

因為成本較高，故一般社區較少安裝門禁系統。目前門禁系統可分成刷卡、指紋辨識、虹膜和人臉辨識等幾種方式，刷卡主要有 Mifare、EM、HID 三種格式。指紋辨識由於社區出入人口眾多，加上辨識率較低，故不太常使用；虹模辨識成本太高，故在社區更為少見，人臉辨識牽涉到個資和隱私等問題，故目前也很少應用在社區。基於上述理由，目前在國內社區最常使用的門禁系統仍以刷卡為主，其中感應扣是最常見的類型。

4. 周晨蕙研究員：請問目前國內建築物內所使用之監控設備和門禁系統，可能會收集哪些個人資料？
5. 張凱強經理：每間公司（保全、物業等）設定的欄位不同，但一般門禁系統會蒐集的個資只有姓名和戶別等，其餘資料與進出管理無關，所以管委會通常不會蒐集。另外，為進行車位管理，門禁系統可能還會蒐集車牌和車位資料。最後，門禁系統可查詢住戶出入時間和進出資料，警政單位可能會跟社區調閱上述資料，這應該也是個資。
6. 周晨蕙研究員：社區住戶或公司員工，取得蒐集處理利用個資之同意較無問題，也比較容易釐清可能會蒐集的個資種類，惟除住戶和員工外，門禁系統和監控設備也會蒐集到訪客資料，這部份目前是如何處理呢？由於訪客往往會蒐集電話、證件等資料，法務部函釋指出，這部份可能有逾越個資法第 5 條比例原則之限制，目前實務如何應對？
7. 張凱強經理：關於訪客的部份，每個社區處理的方式不同，大部分是請訪客填寫登記簿，然後發臨時證件給訪客。由於登記簿的欄位每間物管公司都不同，所以究竟會蒐集到哪些資料，是否有違反個資法限制等，恐怕需要進一步調查。另外，部份商辦或大樓是發臨時卡和臨時 QR code，時間到就會失效，這種作法應該較無後續管理個資的問題。
8. 周晨蕙研究員：綜上所述，目前建築物內無論是一般監視系統或門禁系統的應用類型較為集中，蒐集到的資料類型有限，只是每個社區或大樓的管理政策不同，故實際上究竟會蒐集到哪些資料，是否有確實取得個人同意等，仍然需要進一步調查。在完成資料蒐集後，想進一步請教目前資料管理以及利用的狀況。
9. 張凱強經理：門禁系統或監控設備所蒐集之資料，主要是儲存在設備上，故大多是由物業進行代管。如前所述，由於上述系統所蒐集到的資料有限，加上每個社區智慧化程度不一致，能提供的資料不同，故對於第三者而言是否有用，可能還是要看個案決定。

10. 徐春福執行長：關於資料的部份，我稍微做一些補充。其實現在最嚴重的問題是綁標，設備廠商透過採用特定規格設備（工程完成後難以拆解確認規格）或綁定密碼方式，讓業主難以尋找其他廠商接手維護，導致綁標狀況發生，設備及相關資料都掌握在設備業者手上，真正擁有的資料的業主反而難以直接利用資料。以弱電系統來看，門禁系統有綁的業者約 1-2 成；中央監控則約有 3-4 成綁標。我國目前並無規範要求建築內電梯及弱電系統等採用共通標準及規格，惟我之前曾在柬埔寨參與一個建築採購案，負責該建案之建商要求業者必須公開通訊協定、API 和確保系統相容性，以利業主可以直接進系統撈取資料，我國建商應該要有這種意識，才能達到資料流通和共享之目的。
11. 周晨蕙研究員：謝謝徐執行長和張經理寶貴的經驗分享。目前計畫雖聚焦於安控設備和個人資料問題，惟建築物內有各式各樣的資料，相較於個人資料，這些資料可能更有利用上的價值，惟受限於資料格式等問題，使上述資料難以流通利用。本計畫後續將持續關注智慧建築資料治理和後續利用等問題。

附錄四：台灣星堡保全股份有限公司訪談紀錄

（一） 會議資訊

會議時間：108 年 04 月 1 日 14：00 至 15：00

會議地點：台灣星堡保全股份有限公司

受訪談人：張順轅法務專員

訪談人：周晨蕙

記　錄：周晨蕙

訪談題目：門禁系統及安全監控設備個資運用狀況及問題

（二） 訪談提綱

1. AIoT 發展為我國安全監控產業帶來許多應用機會與挑戰，安控設備可應用於智慧建築、智慧家庭、智慧工廠等不同領域。針對智慧門禁系統和安全監控設備於智慧建築內蒐集資料的狀況，請教以下問題：
2. 智慧門禁系統和安全監控設備之應用情境。

    (1) 智慧門禁系統及安全監控設備蒐集之資料類型，其中是否包含個人資料？
    (2) 智慧門禁及安全監控系統主要會蒐集哪些人的資料？針對訪客或路人，該如何履行個資法上有關告知和取得同意之要求？
    (3) 在蒐集資料的過程中，除個資法限制外，可能還會遭遇哪些困難？如不知道要蒐集哪些資料，故無法確定要安裝哪些設備等。

3. 針對智慧門禁系統和安全監控設備所蒐集資料，後續如何進行保管和處理，請教以下問題：

    (1) 智慧門禁系統和安全監控設備所蒐集到之資料，目前主要是由誰來負責管理？如安裝監控設備之保全業者、物業或建築物管理者（如管委會）。
    (2) 承上，如資料是由保全業者或物業代管，則在更換業

者時，資料會如何處理？

4. 針對資料所有人或第三方想利用智慧門禁系統和安全監控設備所蒐集之資料，請教以下問題：

   (1) 針對智慧門禁系統和安全監控設備所蒐集之資料，請教目前可能有哪些單位想要利用上述資料，以及想要利用的資料類型和應用情境。
   (2) 如果有人想要利用上述資料，目前可能會與哪些單位進行接洽？假使上述單位（如管委會）想要將資料提供給第三方，但這些資料涉及個資，他們可能會以何種方式取得個人同意？

5. 針對智慧門禁系統和安全監控設備所蒐集之資料是否為個資、個資蒐集處理利用之原則和例外，以及個資去識別化等問題，本計畫擬以問答集形式呈現，並透過情境加以描述，使讀者更容易了解。針對上述問答集內容和呈現方式，請教貴公司意見。

（三） 會議記錄

1. 周晨蕙研究員首先說明拜訪目的，為執行「智慧建築安全監控資料應用法制課題及對策之研究計畫」，擬深入了解智慧門禁系統和安全監控設備者個人資料蒐集、處理、利用狀況及困難，對應我國個資法上相關規定及司法實務，找出推動智慧建築資料應用之法制障礙，並針對具體個案編寫問答集，引導及協助業者落實我國個資法遵需求。本次訪談希望能了解國內智慧門禁系統和安全監控設備個人資料蒐集和利用之狀況，作為後續研提法規建議和編寫問答集之參考。
2. 張順轅法務專員：目前門禁系統和安控設備主要應用於住家、商家、公私立學校和公家單位，蒐集資料包含個人資料在內，如：使用人姓名(持卡人)、職稱、住家電話、行動電話、地址、身分證字號、統一編號等，惟實際上究竟會取得哪些資料，仍要看各物業管理方式而定。以本公司來說，我們會在保全服務契約內附上蒐集、處理及利用個人資料告知暨同意書，以書面取得客戶同意，並說明使用目的。
3. 周晨蕙研究員：請問在取得同意的過程中，是否曾遭遇困難？
4. 張順轅法務專員：因目前個資保護意識抬頭，使用者越來越重視個人資料的使用，故要求使用者填寫身分證字號時，常會遇

到不願意的填寫的情況，或是當事人填寫錯誤的資訊。此外，近年來監視系統使用越來越廣泛，保全公司會提供遠端監控等額外服務，如使用者需要該服務，則須另外提供 IP 位址，這個資料可能比較容易被忽略。

5. 周晨蕙研究員：請問後續在資料管理及利用上面，目前的狀況為何？如果都是由保全公司或物業代管，則在更換廠商時，資料會如何處理？
6. 張順轅法務專員：本公司管理的資料，都會統一管理於檔案室內，如有更換業者狀況發生，會簽立三方協議書承接前一業者的權利義務。由於門禁系統和安控設備所蒐集的資料大多是由其他業者代管，所以我認為比較大的問題在於如何監督業者是否落實個資法所要求之安全維護措施。
7. 周晨蕙研究員：針對智慧門禁系統和安全監控設備所蒐集之資料，請教目前實務上是否有利用上述資料之需求？如利用資料進行研發等。
8. 張順轅法務專員：就我所知，我們目前僅碰過配合的軟體商有資料存取及使用的問題，並無其他利用需求。
9. 周晨蕙研究員：關於安全維護措施問題，由於現在這些資料大多都是代管，故該如何透過契約要求業者妥善保管及維護個人資料，會是一個重要的問題，謝謝星堡保全寶貴的經驗分享。

附錄五：台北市政府都市發展局訪談紀錄

（一） 會議資訊

會議時間：109 年 05 月 22 日 16：00 至 17：00

會議地點：台北市政府都市發展局

受訪談人：住宅服務科吳逸民股長、沈珮綺科員、黃慧苓科員；住宅工程科張裕隆正工程司、陳立人副工程司、姜國柱科員

訪談人：周晨蕙

記　錄：周晨蕙

訪談題目：台北市政府社會住宅智慧門禁和安全監控設備運用狀況及問題

（二） 會議資訊

1. AIoT 發展為我國安全監控產業帶來許多應用機會與挑戰，安控設備可應用於智慧建築、智慧家庭、智慧工廠等不同領域。針對智慧門禁系統和安全監控設備於智慧建築內資料應用現況，問答集將區分章節，依照規劃設計、建造、設備導入及應用等階段，蒐集法制相關問題，透過問答集回覆，以利相關人士參閱。針對問答集編排方式及內容，請教下列問題：

   (1) 問答集內擬描述國內智慧建築門禁系統和安全監控設備之應用情境，目前社會住宅已廣泛導入相關系統和設備，請教我國門禁系統和監控設備技術發展和應用範圍。
   (2) 承上，智慧門禁系統及安全監控設備會蒐集許多資料，針對這些資料，後續是否有規劃應用方式？上述資料中可能包含個人資料在內，實務上如何取得個資蒐集、處理和利用之同意？針對訪客或路人，目前又是如何履行個資法相

關規定？

(3) 問答集內擬根據建築物不同階段分章，目前規劃分為規劃設計、建造、設備導入及應用等 4 章，請教有關上述區分方式之意見。

2. 因應國際間重視個資保護和隱私浪潮，陸續有人提倡重視隱私之智慧建築設計理念，而我國「建築技術規則」針對建築物安全維護設計進行規範，並於第 116 條之 4[71]、第 116 條之 5[72]、第 116 條之 6[73]，規定監視攝影裝置、緊急求救裝置和警戒探測裝置之設置方式。上述規定對於建築物之設計有何影響？是否需要進一步明確具體內容？

3. 在大數據時代下，真正的問題在於如何蒐集到足夠多且高品質之資料。從設計和建造觀點出發，門禁系統和監控設備應如何設計和安裝，才能蒐集到足夠的資料？在設計和安裝時，是否會一併考慮如何儲存上述資料及確保資料之安全性？

4. 在設備導入及投入使用後，針對智慧門禁系統和安全監控設備所蒐集資料，後續如何進行保管和處理，請教以下問題：

(1) 智慧門禁系統和安全監控設備所蒐集到之資料，主要是由誰來負責管理（如安裝監控設備之保全業者、物業或管委會等）？市政府和上述業者間是否有就資料之蒐集、處理和保管等事項簽訂契約？

(2) 承上，如資料是由保全業者或物業代管，針對個資部份是否有特別要求業者遵守個資法相關規定（如採取適當之安全維護措施）？此外，由於資料是由業者代管，市政府無法第一時間取得資料，作為資料所有權人，這樣的狀況是否造成後續應用上的不便？

5. 針對資料所有權人或第三方想利用智慧門禁系統和安全監控設備所蒐集之資料，請教以下問題：

---

71 建築技術規則第 116 之 4：「監視攝影裝置應依下列規定設置：一、應依監視對象、監視目的選定適當形式之監視攝影裝置。二、攝影範圍內應維持攝影必要之照度。三、設置位置應避免與太陽光及照明光形成逆光現象。四、屋外型監視攝影裝置應有耐候保護裝置。五、監視螢幕應設置於警衛室、管理員室或防災中心。設置前項裝置，應注意隱私權保護。」

72 建築技術規則第 116 之 5：「緊急求救裝置應依下列方式之一設置：一、按鈕式：觸動時應發出警報聲。二、對講式：利用電話原理，以相互通話方式求救。前項緊急求救裝置應連接至警衛室、管理員室或防災中心。」

73 建築技術規則第 116 之 5：「警戒探測裝置得採用下列方式設置：一、碰撞振動感應。二、溫度變化感應。三、人通過感應。警戒探測裝置得與監視攝影、照明等其他安全維護裝置形成連動效用。」

(1) 針對智慧門禁系統和安全監控設備所蒐集之資料，請教目前可能有哪些單位想要利用上述資料，以及想要利用的資料類型和應用情境。

(2) 承上，如果有人想要利用上述資料進行研發，市政府是否願意提供？是否有單位曾經聯繫市政府申請相關資料？

(3) 承上，由於上述資料涉及個人資料，如欲提供給第三方利用，必須取得當事人同意或將個資去識別化。市政府未來是否會考慮取得個資利用同意或去識別化之方式，以便自己或提供給第三方利用相關資料？

6. 台北市都發局規劃建制台北市公宅管理雲等措施，提供住戶管理和生活服務功能。針對管理雲之運作狀況，請教以下問題：

(1) 業主（市政府）、物業和住戶所需要之資料類型不同，如物業在公寓大廈內主要工作為設備維護、生活服務和人事管理等，住戶東西損壞向物業報修，住戶取得服務後，物業向市政府請款，在這件事中市政府需要的是財務資料，物業需要的是通報紀錄，而住戶要的是維修紀錄，針對上述狀況，目前管理雲如何設計不同的存取權限並進行管理？

(2) 針對資料管理，假使目前是由負責建置管理雲之業者代管，業主（市政府）是否能確實掌握所有資料狀況？未來如有資料應用需求時，是否會有不易取得或資料格式等問題發生？

7. 智慧門禁系統和安全監控設備之資料應用，除個資法外，如持有者為政府機關，亦涉及政府資料開放，以及資料應用方式等議題。請教貴單位是否有關於智慧建築資料應用之問題，可提供研究團隊參考？

（三） 會議摘要

1. 周晨蕙研究員首先說明拜訪目的，為執行「智慧建築安全監控資料應用法制課題及對策之研究計畫」，擬深入了解智慧門禁系統和安全監控設備者個人資料蒐集、處理、利用狀況及困難，對應我國個資法上相關規定及司法實務，找出推動智慧建築資料應用之法制障礙，並針對具體個案編寫問答集，引導及協助業者落實我國個資法遵需求。關於問答集編排方式及內容，研

究團隊目前規劃先於前言說明目前實務狀況，然後再根據建造、規劃設計、設備導入及應用等階段，分別蒐集問題。針對實務狀況及問答集內容，請教台北市政府意見。

2. 吳逸民股長：關於前端建造及要導入那些設備，主要是由工程科負責，住宅服務科會接觸到的後端設備，如防災中心，裡面有視訊監控設備，可掌握社區安全和進行設備監控，確保社區正常運轉。此外，社會住宅內住戶使用門禁系統進出，對講功能可進行視訊，停車場內也有使用車牌辨識和 E-tag 等技術。以上為社會住宅在應用階段，與智慧門禁和安全監控有關之服務及運用狀況，以及可能涉及個資的部份。
3. 周晨蕙研究員：謝謝股長說明，想進一步請教上述系統和設備所蒐集之資料，目前是由哪個單位負責管理及儲存地點。此外，針對這些資料，未來市政府是否會考慮對外出售或提供，以發揮資料的價值？
4. 吳逸民股長：涉及個人資料的部份，都會由市政府這邊管理，物業可能會基於管理需要，持有一些資料，如門禁卡是由哪位住戶持有，以便日後回收，但住戶電話、身份證等個人資料，市政府不會給物業。目前社會公宅所蒐集到之監視器影像等資料，都是儲存在當地的主機內，要取用資料需要登入和具有相關權限，市府也有搭配高規格防火牆，可以確實掌握資料的動向。關於未來是否會對外提供資料等作法，由於個資較為敏感，可能需要多一點研究和討論，至於市政府自己是否有利用資料的需求，我們有在考慮利用門禁系統的資料來優化服務，至於影像資料之利用，目前還沒有進一步想法。如住宅服務科日前徵案公告「社會住宅門禁優化解決方案實證計畫」，便希望能透過分析人員進出紀錄（次數、時間），一般住戶和弱勢戶（如獨居老人）進行頻率、時段，即時發現異常數據，以儘早做出反應。然而，門禁系統蒐集個資之目的在於管理場域進出，並非用於分析，故上述以優化服務為目的之利用，可能需要另外取得住戶同意，市政府也會盡量在與住戶簽訂之契約內進行說明。
5. 周晨蕙研究員：台北市都發局建置公宅管理雲平台，提供住戶管理和生活服務功能，針對平台運作狀況和所涉及之問題，請教市政府經驗。
6. 吳逸民股長：針對公宅管理雲，市政府之前有在研究分析門禁系統資料，以優化相關服務和決策之可行性。然而，真正的問題在於，廠商如何確保在開發過程中，不會有第三人取得資料，並且可透過控管機制，讓想利用資料進行分析者僅取得所需資

料。針對上述問題，我們目前還沒有看到太多案例可以參考，但這部份會是未來我們分析門禁系統資料利用可行性的重點。針對上述問題，建議科法所或許可以進一步聯繫軟體開發商了解細節。

7. 周晨蕙研究員：關於問答集編排，我們擬分成建造、設計等章節蒐集相關問題，針對建造、設計和設備導入等前階段，「建築技術規則」有針對建築物安全維護設計進行規範，並於第 116 條之 4、第 116 條之 5、第 116 條之 6，規定監視攝影裝置、緊急求救裝置和警戒探測裝置之設置方式。考量到未來資料應用需求和個資保護等問題，上述規定是否有需要調整的地方？
8. 張裕隆正工程司：以實務需求來看，其實規定越簡單越好，目前僅要求在停車場出入口、車道等處裝設監視器已經足夠，不太需要增加裝設處所。在住戶方面，其實我們很少會碰到有住戶反應裝設監視器會侵害隱私，反而是有住戶會希望能多在一些地方裝設，以便進行管理。關於監視器部份，除符合法律規定外，我們也會依照機構需求，另外在公共區域進行裝設。針對個資和隱私保障，市政府目前並未接到任何住戶有關個資的客訴，所以這部份應無太大問題。另外，關於建造和設計階段問題，請張立人副工程司及姜科員說明。
9. 張立人副工程司：門禁卡儲存資料包括戶別和 ID，如果有人駭進來竊取資料，就可以複製門禁卡，所以我們都有設置防火牆避免資料外洩。另外，台北市政府都發局出版一本台北市公共住宅智慧社區建置參考手冊，希望能讓各界了解智慧社區之採購、設計、施工、竣工驗收到營運管理等各階段整體架構和操作設計原則，提供給科法所作為參考。
10. 姜國柱科員：另針對監控資料之閱覽補充說明，目前這些資料都只有本局或是檢調機關來文才可以閱覽。
11. 周晨蕙研究員：請問關於系統之操作，以及個資同意等部份，市府會先向住戶進行說明嗎？
12. 張立人副工程司：這部份是由物業向住戶說明，市府則會針對物業進行教育訓練。
13. 姜國柱科員：我們發現物業並不熟悉智慧建築相關系統和設備之操作，這反而是實務上比較容易產生問題之處。
14. 張立人副工程司：另外，針對資料之儲存補充說明。目前儲存在主機的資料，大部分都不會保留太長時間，可能一個月後就會刪除。
15. 周晨蕙研究員：最後請教台北市政府，針對智慧建築相關法制，從實務角度出發，目前有哪些部份覺得是未來需要加強或進一

步釐清的？

16. 張立人副工程司：我目前想到的是人臉辨識問題。美國有許多州已經立法明文禁止使用人臉辨識技術，我國在這部份規範仍不明確，實務上可能會產生一些困擾。其實我們的系統都有規劃類似功能，同時我們會要求廠商必須設計禁用功能，讓業主可以根據實際需求和法規，選擇是否要開啟人臉辨識功能。
17. 周晨蕙研究員：資策會科法所謝謝台北市政府都市發展局寶貴的經驗分享。

附錄六：中華民國全國建築師公會訪談紀錄

（一） 會議資訊

會議時間：109 年 6 月 8 日 10：00 至 11：00

會議地點：中華民國全國建築師公會

受訪談人：鄭宜平理事長

訪談人：王自雄、周晨蕙（職稱略）

記　錄：周晨蕙

訪談題目：從建築師角度看智慧建築監控設備資料應用問題

（二） 訪談提綱

1. AIoT 發展為我國安全監控產業帶來許多應用機會與挑戰，安控設備可應用於智慧建築、智慧家庭、智慧工廠等不同領域。針對智慧門禁系統和安全監控設備於智慧建築之運用狀況，請教以下問題：

   (1) 我國目前智慧門禁系統和安全監控設備之技術現況及應用情境。
   (2) 智慧門禁系統及安全監控設備蒐集之資料類型，以及這些資料未來加值運用之可能性和方式。
   (3) 上述資料如欲釋出利用，可能會面臨資料所有權不明（資料是設備商、建商還是建築物所有人的），以及涉及個人資料等問題。請問目前實務上是否會針對上述資料之歸屬和利用方式等進行約定（如儲存地點與方式，誰負責管理及管理權限等等）？
   (4) 承上，上述資料如由保全業者或物業代管，則會如何避免更換業者後無法取得資料等問題？

2. 因應國際間重視個資保護和隱私浪潮，陸續有人提倡重視隱私之智慧建築設計理念，從資料蒐集和個資及隱私保護觀點出發，未來應如何設計門禁系統和安全監控設備，以兼顧資料蒐集和

個人權利之保護？

3. 承上，建築技術規則規範建築物之安全維護設計，於第 116 條之 4[74]、第 116 條之 5[75]、第 116 條之 6[76]，規定監視攝影裝置、緊急求救裝置和警戒探測裝置之設置方式。以目前智慧建築發展趨勢而言，建築技術規則內相關規定是否有需要調整或加以補充之處？
4. 針對智慧門禁系統和安全監控設備所蒐集之資料所涉法律問題，本計畫擬以問答集形式呈現，並輔以情境描述，使讀者更容易了解。針對上述問答集內容和呈現方式，請教理事長意見。

(1) 關於問答集之編排，團隊擬先在前言介紹智慧建築及門禁系統、監控設備等概念，以及目前實際運用狀況，然後再根據建築物規劃設計、建造、設備導入及應用等階段，蒐集相關法律問題。針對上述編排方式及內容，請教理事長建議。

（三） 會議摘要

1. 王自雄主任首先說明拜訪目的，為執行「智慧建築安全監控資料應用法制課題及對策之研究計畫」，擬深入了解智慧門禁系統和安全監控設備者個人資料蒐集、處理、利用狀況及困難，對應我國個資法上相關規定及司法實務，找出推動智慧建築資料應用之法制障礙，並針對具體個案編寫問答集，引導及協助業者落實我國個資法遵需求。關於問答集編排方式及內容，研究團隊目前規劃先於前言說明目前實務狀況，然後再根據建造、規劃設計、設備導入及應用等階段，分別蒐集問題。針對實務狀況及問答集內容，請教理事長意見。
2. 鄭宜平理事長：我國目前在推動智慧建築，係以獎勵性質為主，如透過方案或智慧建築標章等方式加以推動，尚未以法律加以

---

74 建築技術規則第 116 之 4：「監視攝影裝置應依下列規定設置：一、應依監視對象、監視目的選定適當形式之監視攝影裝置。二、攝影範圍內應維持攝影必要之照度。三、設置位置應避免與太陽光及照明光形成逆光現象。四、屋外型監視攝影裝置應有耐候保護裝置。五、監視螢幕應設置於警衛室、管理員室或防災中心。設置前項裝置，應注意隱私權保護。」

75 建築技術規則第 116 之 5：「緊急求救裝置應依下列方式之一設置：一、按鈕式：觸動時應發出警報聲。二、對講式：利用電話原理，以相互通話方式求救。前項緊急求救裝置應連接至警衛室、管理員室或防災中心。」

76 建築技術規則第 116 之 5：「警戒探測裝置得採用下列方式設置：一、碰撞振動感應。二、溫度變化感應。三、人通過感應。警戒探測裝置得與監視攝影、照明等其他安全維護裝置形成連動效用。」

規範。由於智慧建築尚未以法律加以規範，而現行法有關智慧建築之獎勵，如《都市危險及老舊建築物建築容積獎勵辦法》第 8 條、第 11 條;《都市更新建築容積獎勵辦法》第 11 條等，都是圍繞智慧建築證書或標章給予補助，惟標章或證書均係源自於推動方案，一旦政府放棄推動或改推其他方案，就會出現問題。以我國目前規定來看，目前有關智慧建築之法規只有「建築技術規則」之建築物安全維護設計，以及營建署「智慧建築設計技術參考規範」，要從法規要求建築師在設計時落實個資和隱私保護，僅能透過上述規定為之。

3. 王自雄主任：從目前智慧建築需求和法規來看，有哪些地方是建造設計時需要預做準備的？法規是否需要加強？
4. 鄭宜平理事長：關於智慧建築，我認為不應強調智慧建築，智慧化應該要擴張到智慧社區、智慧城市，乃至於智慧國家。建築物智慧化程度不需要很高，對民眾而言，建築物智慧化程度只要符合住戶需求就好，且不同人和年齡層對智慧化需求及接受度不同，所以建築物智慧化只要設定最低標準，讓設計師可以此為標準進行設計即可。另外，在智慧化設計上，由於前端設備 2-3 年就會汰換，後面的系統不會一直更換，所以重要的是前端的規劃，在設計時要想好如何持續更新設備。綜上所述，回歸您提出的問題，我認為目前的法規已經足夠，不需要多做限制。
5. 王自雄主任：從法律人角度來看，智慧建築所蒐集到的很多資料都涉及個資，所以誰可以取用資料成為重要問題。針對此一問題，我們擬針對「建築技術規則」第 116 條之 4 有關注意隱私權保護之規定，透過指引和問答集方式，更詳細地說明該如何落實法規要求。針對應放進指引和問答集之內容，理事長這邊是否有任何想法或建議？
6. 鄭宜平理事長：個資是一個關鍵問題，科技越發達，隱私暴露越多。關於有沒有應放進指引或問答集內容，這部份或許可以參考智慧建築評估手冊，手冊內針對各項評估項目，都有設定基本和鼓勵項目，建築師在設計時都是依照法規或標章需求進行設計，故可以這些項目為例進行說明。
7. 周晨蕙研究員：針對問答集架構，我們目前預計分為建造、設計、導入設備和應用等章節，蒐集相關問題，請教理事長對問答集架構和編排方式之意見。
8. 鄭宜平理事長：問答集重點在於讀者是誰，比如一般人對於建造和設計可能沒有興趣，這點可能是需要先釐清的部份。
9. 王自雄主任：資策會科法所謝謝理事長寶貴的經驗分享。

附錄七：台灣建築中心訪談紀錄

（一） 會議資訊

會議時間：109 年 9 月 11 日 15：00 至 16：00

會議地點：台灣建築中心

受訪談人：王冠翔組長

訪談人：周晨蕙（職稱略）

記　錄：周晨蕙

訪談題目：我國智慧建築門禁和監控設備應用現況

（二） 訪談提綱

1. AIoT 發展為我國安全監控產業帶來許多應用機會與挑戰，安控設備可應用於智慧建築、智慧家庭、智慧工廠等不同領域。針對智慧門禁系統和安全監控設備於智慧建築內資料應用現況，問答集內分為入門篇、進階篇和案例篇，說明相關問題，針對問答集內容和編排方式，請教以下問題：
   (1) 問答集內針對智慧建築門禁系統和安全監控設備之應用情境，說明可能遭遇的個資問題及注意事項。針對目前問答集內所列之應用情境，是否還有可以補充的地方？
   (2) 承上，關於目前問答集內整理門禁系統和安全監控設備所蒐集資料可能之用途（如下表），是否還有可以補充的地方？
   (3) 問答集目前分為入門、進階和案例三章，請教有關上述區分方式，以及呈現方式之意見。
2. 由於智慧建築相關資料使用上問題，大多出現在應用階段，若想透過法規來避免相關資料之蒐集、處理、利用侵害當事人權益，或促進智慧建築資料應用，或許可以考慮修正《公寓大廈管理條例》，加強管理組織之責任或住戶之義務，如要求住戶原則上不得拒絕管理負責人或管理委員會使用門禁系統或安全監控裝置所蒐集到之資料。針對上述看法，請教王組長意見。

	應用情境	資料類型	資料用途
門禁系統	在建築物出入口設置門禁，個人必須透過刷卡、指紋、虹膜、人臉辨識等方式進行驗證，進入特定區域	使用人姓名（持卡人）、職稱、住家電話、行動電話、地址、身分證字號、統一編號、戶別、車牌和車位、出入時間和進出次數、聲音等個人資料	1. 場域進出管理 2. 掌握特定人進出履歷、時間、動線，用於提供個人化服務 3. 提供給其他單位（如檢調機關）

	應用情境	資料類型	資料用途
監視攝影裝置	拍攝公共區域內影像	公共區域內特定或不特定多數人，以及周遭環境影像資料	1. 場域安全監控 2. 紀錄場域狀況 3. 統計人數 4. 統計性別和年齡等人物特徵 5. 紀錄人物座標和人流動線 6. 統計分析上述資料之間的關聯性 7. 將影像資料與其他資料進行比對 8. 利用影像資料訓練 AI 或進行產品研發

（三） 訪談紀錄

1. 周晨蕙研究員首先說明拜訪目的，為執行「智慧建築安全監控資料應用法制課題及對策之研究計畫」，擬深入了解智慧門禁系統和安全監控設備者個人資料蒐集、處理、利用狀況及困難，

對應我國個資法上相關規定及司法實務，找出推動智慧建築資料應用之法制障礙，並針對具體個案編寫問答集，引導及協助業者落實我國個資法遵需求。關於智慧建築內門禁系統和監控設備應用狀況，以及問答集編排方式及內容，請教王組長意見。

2. 王冠翔組長：目前監視攝影機主要分為兩種用途，一種是單純拍攝場域內影像留存，發生問題後供人調閱，系統通常會設定存取權限和條件；另外一種是拍攝分析用影像，取得影像後會進行分析，得到經分析之資料後會將影像刪除。此外，關於門禁系統資料，目前可能存在保全公司、雲端或建築物內主機，亦即資料是委託他人進行管理。針對上述狀況，問答集是否有進行說明？
3. 周晨蕙研究員：目前問答集內包含上述兩種監視攝影機用途，並針對拍攝影像用於分析狀況進行詳細說明。另外，針對將門禁系統資料儲存在他處，委託他人進行保管之狀況，我們有在問答集內說明委託他人蒐集、處理個人資料之規定。
4. 王冠翔組長分享門禁系統和監視攝影系統連動狀況：門禁系統可以與其他系統連動，以監視攝影系統為例，當住戶刷門禁卡後，攝影機可以紀錄該名住戶特徵，透過每次刷卡不斷紀錄和訓練監視系統，未來就算該住戶沒有刷卡，只要通過攝影機，監視系統也可以判斷現在通過攝影機之住戶是持有那張門禁卡。透過上述技術，未來公寓大廈內管理委員會就可以知道誰在走廊上抽煙或亂丟垃圾，解決公寓內常見的糾紛和抓不到人的問題。
5. 周晨蕙研究員：謝謝王組長提供上述案例，我們會作為問答集內案例分析之參考。
6. 王冠翔組長：最後再針對問答集內容提出兩個建議。目前問答集內沒有提到住戶是否有權利要求刪除資料，從實務角度出發，住戶資料雖然是個資，但這些資料涉及安全紀錄，刪除的話可能會影響目的之達成。此外，門禁如果只是單純用於進出管理，其實不一定需要蒐集個人資料並建檔，建檔通常是有其他需求，如出缺勤紀錄等。
7. 周晨蕙研究員：謝謝王組長建議，根據目前個資法規定，在符合特定條件狀況下，當事人確實可以主張停止利用或刪除其個人資料，我們會再把上述問題納入討論。
8. 王冠翔組長：針對問答集編排方式，建議正文前可新增一張說明問答集使用方式，這樣讀者才知道該如何閱讀，另外亦可考慮新增有關推薦閱讀順序、對象等說明。此外，問答集內部份用語太過艱澀，應考量讀者略做調整和修飾。

9. 周晨蕙研究員：資策會科法所感謝王組長寶貴的經驗分享和建議。

附錄八：工作會議（一）

（一） 會議資訊

會議時間：109 年 05 月 4 日 15：00 至 16：00

會議地點：建研所 13 樓討論室（一）

出席人員：建研所羅時麒組長、許虎嘯博士、吳偉民；科法所王自雄主任、周晨蕙

紀　　錄：周晨蕙

（二） 會議紀錄

1. 羅時麒組長：本計畫手冊架構編排建議參考「綠建築雨水貯集利用系統模組設計手冊」，以規劃設計階段、建造階段、設備導入/應用階段和使用階段進行區分，分成不同章節，每章介紹與各階段相關之個資問題。由於本計畫目標為編寫問答集，請盡量蒐集 30 個以上問題，豐富問答集內容，並於 6 月召開小型座談會，向專家請益。
2. 徐虎嘯博士：「永續智慧社區實證場域推動策略及法制建構計畫」曾經對實證場域所面臨之個資問題進行盤點和分析，建議本案可參酌並納入作為參考。另外，本計畫應先盤點建築相關法令與個資和監控設備等相關規定,如建築法、建築技術規則、公寓大廈管理條例等。最後，在訪談對象上，由於目前受訪對象多為設備業者及系統整合商，建議增加規劃設計階段之建築師、業主，以及終端之消費者（如住戶、個人等），方能全面性掌握可能存在之問題。
3. 吳偉民：「建築技術規則」第 116 條之 2 有規定全維護裝置設置區域，可從此處出發，說明在各種設置情境上可能需要考量的問題。另外，手冊中亦可補充相關函釋。
4. 王自雄主任：本計畫將參考上述建議，在架構上將依照規劃設計、建造、導入及使用等階段進行編排，並針對不同階段尋找 1-2 位以上受訪者，透過訪談等方式，蒐集各階段相關個資問題。此外，配合防疫需求，本計畫會儘快規劃於 6 月舉辦小型座談會。

附錄九：工作會議（二）

（三） 會議資訊

會議時間：109 年 09 月 26 日 15：00 至 16：00

會議地點：建研所 13 樓討論室（一）

出席人員：建研所羅時麒組長、許虎嘯博士、吳偉民；科法所王自雄主任、周晨蕙

紀　　錄：周晨蕙

（四） 會議紀錄

1. 徐博：先說明本計畫問答集草案各版本差異。前兩版以文字為主，但用語較為艱澀，故建議修正以圖表為主，以利讀者理解。科法所目前已經將問答集內容轉換為 Q&A 形式，本次工作會議要確認架構和內容。另外，本計畫需求書為提出草案，想確認草案是否需要經過美編？
2. 羅組長：草案係指經審查內容無誤後，可以拿去出版社印刷，故仍需簡單的排版，但版面是否美觀其次，重點是內容要淺顯易懂。目前草案全部轉換為 Q&A 形式，但用語定義和基本概念說明等部份無須用 Q&A 方式呈現，部份涉及法律用語之定義，應指出法規依據，才不會讓人誤會是本所提出新定義。目前 Q&A 很多是有關某類型資料是否為個資之說明，以及這樣的處理方式是否為個資法上之處理，建議可將這些基本概念之說明，全部都整併到後面案例說明，讓讀者可以直接從案例看起。另外，關於智慧建築門禁系統和監視攝影裝置之應用情境，可以參考本所今年剛發行之手冊。
3. 羅組長：問答集以 16 開大小進行設計，無須將全部內容轉為 Q&A 或圖示，以案例為主進行說明，至少舉出 10 個應用情境。
4. 王自雄主任：本計畫將參考上述意見，重新調整問答集架構和內容，前言、使用說明和基本概念說明等部份，會調整回以文字描述的方式；Q&A 部份將全部改為以案例為主，將目前 Q&A 內容融入案例中進行說明。

附錄十：智慧建築安全監控資料應用法制對策問答集座談會會議紀錄

（一）會議資訊

會議時間：109 年 7 月 9 日上午 10 時 00 分至 12 時 00 分

會議地點：內政部建築研究所

與會人員：吳逸民、陳立人、楊勝德、陳遠鴻、黃朝信（代理）、游璧菁（代理）、張中傑、林世俊、羅時麒、徐虎嘯、吳偉民、王自雄、周晨蕙、鄧佩琳（職稱略）

記　　錄：周晨蕙

（二）會議記錄

1. 王自雄主任說明今日座談會討論提綱和目的，希望與會各位專家惠賜意見。
2. 羅時麒組長：現在大眾十分重視個資和資安等議題，時常有人詢問在導入智慧化設備時該如何配合法規要求，所以我們希望能透過這個計畫，採取由下到上方式，廣泛蒐集個案法律問題，以順利推動建築物智慧化，並協助產業界發展。
3. 周晨蕙法律研究員進行引言簡報，本次議題主要報告計畫執行狀況，以及根據訪談結果和參考國外文獻後提出之問答集草案規劃，並針對草案內容請專家給予建議。
4. 台北市政府都市發展局住宅服務科吳逸民股長：台北市都發局負責管理維運社會住宅，針對管理層面需求，目前實務上比較常遇到的問題包括監視器設置位置和數量、資料取用方式，以及資料能否進一步分析利用等。針對上述問題，本局目前係根據《建築技術規則》要求，僅在主要進出口設置相關設備，但都發局在社會住宅上同時具備房東和管委會的身份，必須介入排解住戶糾紛，故社會局目前考慮在各層門廳出入口增設監視器，在不侵犯隱私的前提下（如監視器不拍攝住家大門），盡量掌握住戶動線，否則可能會有人抗議都發局無法找出造成問題的住戶。另外，針對門禁部份，社會住宅和傳統公寓大廈一樣，都是委託物業公司管理，但社會住宅有 30%住

戶是低收入戶和獨居老人，雖然社會局會定期訪視關心住戶狀況，但也曾經差點發生憾事，只靠物業公司管理和社會局訪視可能無法即時掌握住戶狀況，所以都發局想要透過分析門禁系統資料，了解住戶出入狀況，設定條件提醒管理人員（如某住戶已經很久沒有出現），避免憾事發生。

5. 台北市政府都市發展局住宅工程科陳立人副工程司：住宅工程科負責社會住宅內機電設備整合及導入，目前門禁系統除出入口外，還會設置在機房，住宅單元則因個人隱私考量，只有設置電子門鎖，且除非有特別情況（如有外人闖入），原則上不會與中央監控系統連線。在監視器設置上，目前有住戶希望能增設監視器（《建築技術規則》僅規定建築物出入口、停車場出入口等處必須裝設，其他部份保留彈性），我們也在思考該如何設置，希望能平衡設計端和住戶需求，避免拍攝到住宅內部。另外，目前門禁系統有預設人臉辨識功能，只是考量到其他因素沒有啟用，未來我們會再與住宅服務科討論，是否只要經住戶同意，就可以改由人臉辨識進行出入管制。
6. 王自雄主任：在建築物不同階段，通常前端的管制性較強，故會透過《建築技術規則》加以規範，明定建築物應如何設計和建造，但後端的管制性較弱，較適合透過指引性規定引導形成秩序，減少在使用過程中可能產生的疑慮。
7. 台北市建築師公會黃朝信建築師：關於今天的課題，《建築技術規則》內目前只有針對安全監控設備加以規範，未來或許可以針對不同建築物類型內之門禁和安全監控設備，訂定相應之技術規範，並導入個資保護相關課題。以社會住宅和集合住宅為例，社會住宅業主身兼房東和管委會角色，有管理和利用資料優化服務之需求，針對門禁和監控設備所蒐集資料的管理權限，未來應考慮加以規範。
8. 王自雄主任：以我們的經驗來看，問答集往往可以發揮比想像中更大的效果，有助於形成業界共識，之後再將指引轉為強制性規範所受到的阻力會較小，推動上也會更加順利。另外，由於個資法屬於操作性很強的規範，必須搭配具體情境和案例，才能知道該如何適用，謝謝黃建築師從建築物類型切入，給予我們具體建議。
9. 中華民國全國建築師公會楊勝德建築師：安全監控設備範圍很廣，包括人員監控和設備監控在內，建議問答集將範圍限定在人員監控，並於標題註明「智慧建築人員安全監控」，以避免誤解。另外，

在建築物規劃設計之初，都是針對硬體設備進行規劃，等到工程快完成時，才會導入機電等相關設施，由於設備導入為建造後期階段，要透過《建築技術規則》規定應導入哪些設備和作業方式，恐怕會有困難。然而，有關資料的存取權限和管理方式等，或許可以考慮透過《公寓大廈管理條例》加以規範。

10. 新北市建築師公會陳遠鴻建築師：根據《建築技術規則》第 116-1 條，安全維護設計相關規範僅適用公共建築物，換言之，只有公共建築物才需要加裝安全監控設備，未來或許可以考慮增加其他建築物類型和設置空間。目前《建築技術規則》亦未明定監視器總機設置位置，未來總機應設於防災中心（高樓層大樓需設防災中心）或管理員室，亦可考慮明確加以規範，並增加有關監控資料存取和控制，以及不斷電系統（能容許安全監控設備斷電多久）等規定。最後，近來悠遊卡發生複製儲值爭議，為避免同樣問題發生，如使用磁卡作為門禁，可能也要考慮針對磁卡進行管理。
11. 周晨蕙研究員：針對監視器等安全維護裝置，目前《建築技術規則》內規定較為簡略，僅規定公共建築物必須加裝相關裝置，且僅要求設置在特定空間(如大樓出入口)，無法滿足建築物管理需求。然而，由於監視器要設置在哪裡涉及住戶需求，難以在事前透過《建築技術規則》加以規範，故藉由問答集告訴設計者或管理者，未來如有類似需求時，可以考慮在哪些地方加裝監視器及保存、處理資料，或許是比較妥當的作法。
12. 生產力建設張芳民總經理：從建商角度來看，科技發展是必然的，不能因為擔憂法規限制而不去布建相關設施，重點在於需釐清蒐集資料目的在於服務管理還是監控，服務管理對民眾有利，使用者較不會抗拒。建築物社群內有兩大體系：物業管理和生活服務，前者相對單純，而後者涉及私領域非常複雜。建築物內必須將公領域和私領域分開討論，公領域相關規範越標準越好，但在資料方面，最需要管理的應該是物業。
13. 王自雄主任：其實個資和隱私等問題一直存在，重點在於這些問題為什麼現在受到重視。謝謝張總經理給予的建議，不管觀念是否轉變，法規環境如何變化，都不能因此阻礙進步，仍應完成相關設施布建，避免日後無法跟上時代腳步。科法所也一直協助政府機關，找出影響技術發展之法制障礙，以促進相關產業發展。

14. 游壁菁副理事長：首先，本問答集標題為「智慧建築安全監控資料應用」，建議思考是否使用「監控」兩字，因為監控等用語可能會造成使用者牴觸心理，由於建築物導入智慧化設備目的在於提供服務，故建議可思考如何調整用語。其次，本問答集設定對象為使用者，對使用者而言有兩件事非常重點，第一個是能透過問答集排除使用者疑慮，第二是讓使用者知道智慧建築透過蒐集分析、應用資料，才能享受相關服務。最後，智慧建築目前蒐集非常多資料，但我們擔心的是資料沒有被妥善運用，應該要讓使用者了解資料可以用於優化管理服務，分析和排除潛在危險，達到防範於未然之目的。如此一來，相信可以有效降低使用者疑慮。
15. 王自雄主任：服務品質的提高和優化，與個別化息息相關，必須要讓使用者認識到這一點。此外，用字用語會影響使用者感受，我們也會多加注意。
16. 張中傑秘書長：在目前智慧城市發展趨勢下，許多建築物在規劃設計階段就會導入安全監控設備，相關資料通常是由物業進行保管，故應針對物業和實際管理資料的人加以規範。
17. 林世俊常務監事：首先應討論蒐集資料之特定目的，可從建築物安全營運管理和服務行為之必要性出發，惟因應建築物使用類型，可能還需要再進一步細分，並考慮是單一所有權人還是區分所有權人等問題。惟不管蒐集目的為何，未來在管理上都應取得住戶同意（如透過規約或簽署同意書等方式），才能避免後續發生糾紛。其次，門禁系統所蒐集到資料應區分為數位資料、生理特徵資料和影音資料（包括錄音和影像）等，並應要求在編輯應用上述資料時，不能竄改原始資料。此外，目前取得合格級以上智慧標章建築物，監視器都含有錄音功能，簡報 p.13 所列資料沒有錄音檔，建議將錄音檔納入。接下來，因應雲端化發展，異地備援和管理等問題將越來越重要，目前問答集僅就單一建築物狀況加以討論，未來可考慮納入上述狀況。以我個人參與智慧型辦公大樓經驗為例，目前會利用影像辨識訪客，可以減少訪客等待時間，提高服務滿意度，同時計算各層人流，以利規劃逃生疏散路線。上述服務為必然發展趨勢，但重要的是原始資料的保存和維護，不能被竄改，且從第一線人員到高層都應被管控，避免資料外洩。
18. 王自雄主任：針對以法律規範門禁資料及相關人員建議，我們會思

考如何納入現行法體系。其實針對原始資料和相關人員之規範，我國個資法已有相應規定，惟個資法及相關規範與實務間仍存在相當大的落差，本計畫嘗試透過制定問答集，拉近法規和實務之間的距離。

19. 羅時麒組長：本計畫為「智慧化居住空間整合應用人工智慧科技發展推廣計畫(2/4)」底下之子計畫，重點在於推廣建築物應用人工智慧科技，建議計畫團隊納入人臉辨識等議題，並將焦點集中在建築物。簡報 p.26 規劃依照《建築技術規則》將建築物分為 9 大類型，依序整理相關應用情境和問題，惟建築物類型繁多且部份類型私人性質較高，建議今年先以通案研究為主，並以供公眾使用建築物為優先。此外，從剛剛各位專家分享經驗來看，目前技術上都沒什麼問題，但隨著技術進步，管理觀念和建築物內管制措施都需要跟著改變，建議計畫團隊了解業界作法，尤其是會面對國際訪客之跨國性大廠，蒐集最新的管制措施。最後，剛剛台北市政府都發局分享關於社會住宅問題，未來社會住宅將有 20 萬用戶，這是無法避免也需要處理的問題。
20. 徐虎嘯博士：《建築技術規則》是規範建築物設計和設置等面向，但很多問題其實出在管理層面，所以應該透過《公寓大廈管理條例》加以規範，讓大家知道管理面應該怎麼做。另外，用語方面建議計畫團隊考慮是否不要使用監控，改為安全管理，以降低使用者疑慮。最後，在問答集呈現方式，建議先針對不同建築物類型進行分類，依照建築物類型區分使用目的，從使用目的出發，讓使用者知道蒐集資料可以達到哪些目的，最後再針對法律問題進行分析。
21. 張芳民總經理：最後補充說明，智慧建築之管理層面非常重要，應該要讓使用者知道蒐集資料是為提供服務。
22. 王自雄主任：謝謝各位專家提供的寶貴經驗和建議。

附錄十一：「智慧建築安全監控資料應用之法制課題及對策之研究」委託研究計畫案審查意見及廠商回應一覽表

項次	評選委員意見	廠商回應
1	智慧建築涵蓋面廣，涉安全監控設備等內容，為什麼只研究智慧門禁及安全監控？原因為何？	本委託研究案係以「智慧建築安全監控資料」於應用面之法制課題及對策為研究對象，故研究範圍謹先聚焦於智慧門禁及安全監控等應用類型。
2	安全監控設備是否包含整合式電線杆，其涉及之法令有哪些？	智慧路燈為發展智慧城市之基礎，包括監控設備、空氣監測、電子看板等應用，不一而足。智慧路燈上所裝設之監控設備，如應用於建築物內部，亦為本計畫所研究之對象。
3	請問虹模、臉部辨識等技術於國內研究及應用之進展？貴會是否有蒐集掌握以利本研究案之應用。	資策會科法所作為科技及產業政策之法制智庫，持續保持與產業界互動，以即時掌握產業趨勢及技術發展動向。關於臉部辨識技術，國內知名廠商訊連科技於 2019 年 3 月舉辦之 FRVT 臉部辨識測試大賽取得第 18 名，辨識速度更高達全球第 3，顯見我國深具相關技術及應用發展之潛力。
4	服務建議書 p.13，研究經費之配置（五）其他費用：其中「委託專業機構針對國內建築物門禁系統及安全監控設備資料蒐集、處理及利用現況進行調查，金額 30 萬」，何以服務建議書未有章節載述「分包計	考量本計畫之研究對象、範圍及規模，相關調查或可由研究團隊自己執行，後續將一併調整計畫經費編列。

	畫及分包單位明細及計畫管理能力說明」？	
5	智慧建築安全監控之應用，將會涉及個資法第 2 條用詞定義哪些個人資料之蒐集：特徵或指紋？	由於個人資料種類繁多，故個資法第 2 條第 1 款「個人資料之定義」除例示日常生活中經常被蒐集、處理及利用之個人資料外，並於同款後段規定「其他得以直接或間接方式識別該個人之資料」為個人資料。有鑑於此，智慧建築安全監控之應用可能涉及哪些個人資料，必須經過實際調查，了解目前實務所蒐集之資料是否得以直接或間接方式識別出特定個人後，方能進一步確認。
6	服務建議書 p.8，p.12-13，人力配置：主持人 1 人參與 1 月、助理研究員 1 人參與 2 月、派遣人力 0.5 人月、對應於服務建議書 p.14 研究進度，於提交期中、期末及成果報告前個階段，分別投注多少人月？	本計畫將於決標後，依委員意見將各該階段投入之人月提供委辦機關參考。
7	資策會科法所主要業務，其中「7.規劃、建置與推行台灣個人資料保護與管理制度（TPIPAS）與資料隱私保護標章（dp.mark），並協助政府機關就內部及所管產業訂定資訊安全暨個人資料保護相關規範。」與「8.協助企業建立法令遵循、內機內控、資訊安全、個人資料管理制度」，有無那些具體成果可資應用於本標案；擬定個資法（第 27 條及其施行細則第 12 條等）關於「…保	資策會科法所數位創新中心在經濟部指導下推動 TPIPAS 制度，協助組織以「PDCA 方法論」建立一套將個人資料與組織營運連結之系統化管理制度，作為核發目前資料隱私保護標章（dp.mark）之依據。 根據個資法第 27 條及施行細則第 12 條規定，非公務機關保有個人資料者，應採行適當之安全措施，由於該措施為自主性措施，故各組織所訂定

	有個人資料檔案者，應採行適當安全措施之明確標準」？	之安全措施可能略有不同。科法所除曾於 2015 年協助經濟部商業司訂定「網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法」外，亦將根據推動 TPIPAS 制度之實績及智慧建築產業需求，參酌「中央目的事業主管機關依個人資料保護法第二十七條第三項規定訂定辦法之參考事項」等規範，適時研提適用於我國智慧建築安全監控資料應用之安全維護措施。
8	資策會科法所有無經個資受有損害之當事人（以書面）授予（訴訟實施權）提起損害賠償訴訟之實例？（個資法第 32、34 條）	依照資策會科法所之組織定位，僅能從事通案性之法制規畫及法律諮詢，故無代表受害當事人提出個資訴訟之經驗。
9	對現況問題之了解及對策之初步看法，宜有更深入探討。	感謝委員建議。本研究團隊將透過深度訪談掌握現況問題，並據以作為研提對策之重要依據。
10	對國內外現行法制措施之檢視及研修建議，對預期研究成果宜有更明確之期許。	感謝委員建議。針對預期研究成果，本計畫將編寫問答集以利業者遵循。另針對我國相關法令之研修動態，如國發會擬於 2020 年推動個資法修法、研擬個資保護專責機構組織法，以及制定開放資料專法等，本研究團隊亦將同步關注並適時研提建議。
11	有關工作小組初審意見，指出研究人力配置、研究人員參與本計畫工作月數及酬金、其他費用之辦公室租金及水電費等須調整修正一節，請提出說明，並提請討論。	本研究團隊(王自雄主任、周晨蕙研究員)係本會正式聘僱之專職員工，依計畫經費規模及投入人月數試算人事費用，係實際所需之人事成本。本研究團隊負責整個計畫執行期間所有相關工作，惟本會並無兼任之人力編制，

12	本案預定執行期間自決標日起至，109 年 12 月 31 日止，請說明參與本案人員係屬專任或兼任。	故以投入之人月數試算其成本。另，辦公室租金係本會向國泰租用，而由科法所使用之辦公室租金費用，依成本分攤方式按計畫投入人月數分攤租金成本，亦為實際產生之費用。 本研究團隊(王自雄主任、周晨蕙研究員)係本會正式聘僱之專職員工，依計畫經費規模及投入人月數試算人事費用。本研究團隊負責整個計畫執行期間所有相關工作，惟本會並無兼任之人力編制，故以投入之人月數試算其成本。
13	有關智慧建築導入人工智慧、遠端監控等資料應用可能面臨的法制課題，開發者、使用者及操作者等大多不甚了解，建議針對相關情境編輯成問答集，供各界參考。	感謝委員建議。本計畫將根據進度規劃深度訪談，以掌握智慧建築導入相關應用之現況，並按使用情境編寫問答集，供各界參考。
14	本案訪談對象限於專家及業者，建議擴大至產學研各界及使用者。	感謝委員建議。本計畫將納入產學研各界及實際被蒐集資料之個人，以利全面了解實際狀況。

附錄十二：期中審查會議審查委員意見及廠商回應一覽表

委員	審查委員意見	廠商回應
廖委員惠燕	建議報告內可增加我國和歐盟、日本個資相關法令之比較。如尚有其他國家法令，建議一併納入，以作為後續研究參考。	期中報告已經簡述歐盟、日本和我國個資法規範，期末報告內會加強有關比較法之論述。
	問答集對象可涵蓋一般民眾及業者。	謝謝委員意見，問答集會調整適用對象與範圍，將業者納入。
	本研究目前訪談對象多為保全相關專業人員，建議可增加使用端，如台北市政府都發局社會住宅已有許多實際入住案例，可訪談該局了解目前執行問題。	本計畫已於109年5月22日訪談台北市政府都發局，並邀請都發局出席專家座談會給予建議。
史委員維斌	有關國外應用法制政策及案例，目前僅提供歐盟和日本相關研究，建議加入其他先進國家執行狀況供參。	謝謝委員建議，期末報告內將補充國外法制及案例。
	目前問答集規劃之建築物類型較多，建議整理歸納應用情境及問題，將問題相同者予以整併，毋需侷限於《建築技術規則》所列之建築物類型。	謝謝委員建議，問答集將整理歸納應用情境，重新檢討案例分類方式。
朱委員曉萍	問答集受眾設定，除一般消費者外，建議可納入業者視角，讓相關業者可以有所依循。	謝謝委員意見，問答集會調整適用對象與範圍，將業者納入。
	關於問答集規劃之案例分類方式，建議可予以簡化，避免用使用服務目的進行分類。	謝謝委員建議，問答集將整理歸納應用情境，重新檢討案例分類方式。
陳委員嘉懿	對照本計畫預期成果第一項，應為實際案例及資料類型之蒐集，但第4章初步成果及附錄訪談所呈現的僅為廣泛的問答討論紀錄，未進一步就其中所談論到的案例、資料類型、參考規範	謝謝委員建議，本計畫會於期末報告內補充有關應用情境、案例和資料類型之說明，並於問答集內列出所涉及之法律問題、參考條文和函釋。

	及建議加以歸納整理。	
	針對預期成果第二項，對應第二章主要提到法令為《建築技術規則》,《建築技術規則》為建築師及建築物建造設計階段規範，應非法制障礙檢討重點，建議應更廣泛建築營運階段牽涉之法令加以探討，對應歐盟及日本法制措施，由資安管制上位機關加以規範，才能制定合乎系統軟硬體業者、空間管理使用單位認可內容。	謝謝委員建議，惟本計畫和問答集係檢討個資利用相關法律問題，並非資訊安全法制，謹先說明。 由於《建築技術規則》為設計階段規範，而個資問題多發生於使用階段，故本計畫後續將以《公寓大廈管理條例》等規範作為檢討重點。
	針對預期成果第三項問答集部份，建議於此階段應規劃使用對象及情境、章節架構，並檢討以建築物類型區分之必要，目前智慧建築以住宿類和非住宿類區分。	謝謝委員建議，問答集將整理歸納應用情境，重新檢討案例分類方式。
	安全監控設備設置位置建議應有法令依據，如哪些位置不適合設置。	謝謝委員建議，惟考量到私人空間是否設置相關設備，恐難以法律加以規範，且目前《建築技術規則》亦已規定應設置和得視需要設置安全維護裝置之公共空間，故本計畫擬透過問答集釐清法律適用上之問題。
欒委員中丕	本案針對建築技術規則設計施工篇第 116 條之 4 第 2 項提出修正條文及具體作法，完成後可供納入修法參考，但建築技術規則著重於建築技術層面，對於監控設備之使用、蒐集及資料之保護處理等，並非建築技術規則規範事項。	謝謝委員建議，鑒於《建築技術規則》著重技術層面，而個資問題多發生於使用階段，故本計畫後續將以《公寓大廈管理條例》等規範作為檢討重點。
	有關安全監控資料之應用及保護處理問題，應為一共通性原則，建議可延定指導手冊，供建築物使用者參考。	謝謝委員建議，本計畫會整理安全監控資料應用相關問題，並透過問答集方式釐清業者和使用者疑慮。

楊委員欽富	智慧建築安全監控資料，使用端為研究重點。	謝謝委員建議，本計畫會將研究重點放於使用端，俾利從使用者角度出發制定問答集。
	訪談對象可增加台灣建築中心。	謝謝委員建議，本計畫會增加訪談台灣建築中心。
	法制障礙分析部份應再加強說明。	謝謝委員建議，本計畫後續將以《公寓大廈管理條例》等規範作為法制障礙分析之重點。
	健康、安全、防疫等議題可納入討論。	謝謝委員建議，針對健康、安全、防疫等議題，本計畫將根據問答集適用對象及範圍，規劃是否納入討論範圍。
中華民國全國建築師公會	安全監控設備範圍很廣，包括人員監控和設備監控在內，建議問答集將範圍限定在人員監控，並於標題註明「智慧建築人員安全監控」，以避免誤解。	謝謝委員建議，本計畫將依據委員意見，調整問答集適用範圍。
	由於設備導入為後階段，要透過《建築技術規則》規定應導入哪些設備和作業方式，恐怕會有困難。有關資料的存取權限和管理方式等，或許可以透過《公寓大廈管理條例》加以規範。	謝謝委員建議，本計畫將參考委員意見，後續將以《公寓大廈管理條例》等規範作為法制障礙分析之重點。
台灣建築中心	本研究透過文獻分析及訪談方式，彙整智慧建築安全監控資料應用在法制上可能遭遇的問題，並提出因應對策及課題作為智慧化應用之參考。	謝謝委員意見。
	建議後續可就門禁系統及安全監控系統資料庫中，列舉相關實務應用情境作為本研究問答集之案例參考，例如社區公共空間門禁系統人流分析，作為冷氣開放時段的節能優化管理、垃圾間開放時段管理等。	謝謝委員意見，問答集內會規劃案例篇，以情境方式說明可能遭遇的問題。
	本研究期中報告符合預期成果。	謝謝委員意見。

附錄十三：期末審查會議委員意見及廠商回應一覽表

委員	審查委員意見	廠商回應
練委員文旭	考量產業實務建議增加：公共區域監視器，如拍到私人場域門口或窗戶，是否侵犯個人隱私？納入問答集草案。	謝謝委員建議，將於問答集內增列相關問題。（問答集問題十二）
	越來越多場域應用 AI 影像辨識，建立不受歡迎之黑名單或 VIP 客戶並進行處置和回應，是否有個資疑慮？	謝謝委員建議，將於問答集內增列相關問題。（問答集問題十）
	問答集第一題目漏列請補正。另目錄只是列出問題內容，不易查詢，建議予以分類或摘要，以利查詢。	謝謝委員建議，問答集已重新調整格式和目錄呈現方式，以便利讀者閱讀使用。
	問答集第 4 題關於住戶要求保全提供觀看影像有違反利用之疑慮等說明，是否有合法的方式建議？如訂定社區公約經區分所有權人同意通過。	謝謝委員建議，因內政部並非個資法主管機關，且很多情境需要個案判斷，故問答集內並未提供明確答案。惟研究團隊會再重新檢視內容，盡量提供明確答覆或建議，以便利讀者參閱。（問答集 p.33）
江委員哲銘	本研究完成國內外建築物門禁系統及安全監控設備之蒐集及案例資料分析。	謝謝委員意見。
	本研究經整理歐盟、英國和日本有關安全監控設備或個資保護之法制和具體措施；完成我國個資法籍相關規定對於智慧建築	謝謝委員意見。

	安全監控資料應用之法制課題分析。	
	本研究亦已完成智慧建築資料應用法制障礙及因應對策問答集，研究成果值得肯定。	謝謝委員意見。
	建議可作成提出法制課題及對策彙整之結論。	謝謝委員意見，本計畫將於成果報告第四章補充結論與建議。（成果報告 p.41）
陳委員 嘉懿	針對本案之法制課題對策，除直接導向問答集的編寫及出版作為民眾指引外，是否可先提出上位的對策架構，作為本課題發展藍圖及後續推動之方向建議。	本計畫將參酌委員建議，於成果報告內補充有關發展藍圖及後續推動方向之建議。（成果報告 p.20）
	問答集目前定稿版本雖求讀者友善，採情境敘述方式，但在問題 QA 索引上較不直接，仍建議保留原有 QA 於附錄，以求解答效率。圖片呈現方式，可參考報告中日本作法，以照片場景加註。	問答集已重新調整格式和目錄呈現方式，以便利讀者閱讀使用。 在圖片部份，目前問答集內所附圖示均係在解說概念，故未使用實際場景照片。如之後問答集內容調整，有使用照片說明之需要，會參考日本作法，以增加臨場感。
	建議問答集附錄可提供 p.17 所述之公寓大廈規約範本中針對本議題之建議，及資料提供第三方使用時之契約範本，以便民眾參考，協助權益保障。	謝謝委員建議，因內政部並非個資法主管機關，且公寓大廈規約範本係由主管機關訂定，故問答集內並未提供明確答案。惟研究團隊會再重新檢視內容，盡量提供參考條約，以便利民眾參閱。（問答集 p.33）
	情境中是否可以加入對門禁、CCTV 設備建置廠商避免觸法之建議。	謝謝委員建議。惟資料取得及利用之合法性問題，不一定與相關設備建置地點或位置有關。如要提供廠商建議，或許未來可參考英國作法，提供 checklist 供廠商確認。

欒委員中丕	有關將建築技術規則建築設計施工篇第 166-1 條至第 116-7 條視為智慧建築之最低標準一，考量同規則建築設備編第 8 章與本案更具關聯性，其中第 138 條-1 列出相關管理監控設備，建請納入檢討。	謝謝委員建議，本計畫已修正相關論述，刪去視為智慧建築最低標準等描述（成果報告 p.6），並一併調整問答集草案前言。
	有關個人資料保護法及相關法令條文規定，對於本案運用個人資料各階段的關係及規範事項，建議可考量補充分析。	謝謝委員建議，本計畫前兩版問答集原係依照資料應用流程分析所涉問題，惟經工作會議討論認為該分析過於側重個資法，故將該篇章移除。有關個資法各階段所涉議題，可參考附錄十五和附錄十六。
台灣建築中心	本案從智慧建築之門禁系統及安全監控設備角度探討資料應用之法制層面課題與對策，對日後建築數據資料彙集分析有極大參考價值。	謝謝委員意見。
	建議將訪談與分析結果於研究成果章節中彙整收斂，呈現不同情境之因應對策與注意事項。	本計畫將參酌委員意見，於成果報告內調整架構和新增內容。（成果報告 p.14-17）
	建請於摘要中納入最終研究結論。	謝謝委員意見，本計畫將於成果報告第四章補充結論與建議。
	附錄十三部份頁首顯示為附錄十二；附錄部份文字框內文字編排不完整。	謝謝委員意見，本計畫將於成果報告一併調整格式。

附錄十四：問答集草案第一版

壹、前言

伴隨時代進步，物聯網、大數據、人工智慧等新技術開始應用於建築物，衍生許多創新應用服務。智慧化居住空間之創新應用，例如智慧門禁系統、安全監控系統、健康照護，空調、照明、電梯等設備之節能管理等，可透過聯網設備或感測器蒐集個人生理及日常活動資料，以及設備使用狀況等數據，用於完善及提供相關服務。然而，由於個人生理資料或日常活動資料等，可能該當我國個人資料保護法上之個人資料，導致一般民眾對上述應用感到不安，加上歐盟一般資料保護規範（General Data Protection Regulation, GDPR）施行後，加強對歐盟境內個資蒐集和利用之保護，亦影響到其他與歐盟有交易往來之國家，使得智慧建築資料相關法律問題變得越來越複雜，成為業者於建築物內導入相關應用之阻礙。

我國目前有關智慧建築之規範，以獎勵性質之智慧建築標章為主，內政部並訂有「智慧建築設計技術參考規範」，就各類型建築物智慧化之共通部份，依設置標準加以分級規範，提供給智慧建築起造人、設計人、各專業技術及相關機關參考。除上述獎勵性標章及參考規範外，《建築技術規則》建築設計施工篇第四章之一「建築物安全維護設計」針對供公眾使用建築物之公共空間設置安全維護裝置設有規範，而上述安全維護裝置，如照明裝置、監視攝影裝置、緊急求救裝置和警戒探測裝置等，與智慧建築標章和「智慧建築設計技術參考規範」之安全防災指標相仿，故應可將《建築技術規則》有關建築物安全維護設計之規定，視為我國法上有關智慧建築之最低標準。

上述安全維護裝置中，由於監視攝影裝置會蒐集影像等個人資料，屢屢成為輿論關注重點。本問答集經訪談和舉辦座談會，徵集台北市政府都市發展局、保全業者和設備廠商、建商、建築師公會、智慧建築協會、物業管理學會、保全商業同業公會等產學研各界意見，發現利用門禁系統或監視攝影裝置資料，提供及完善建築物內部各項服務之需求與日俱增，如分析獨居長者平常進出大門時間和頻率，掌握住戶安全，避免獨居長者發生意外卻無人知悉等狀況發生。此外，對業者而言，由於業界普遍不熟悉個資法相關規範，可能會因為擔心蒐集及利用資料違反個資法，而影響其於建築物內導入相關設備之意願；對於一般民眾而言，可能會因為不清楚資料提供給誰、如何處理和利用資料、提供後資料將用於何處、對提供資料的人而言有什麼好處等問題，使其過於擔心個人資料被濫用而感到不安。

綜上所述，為鼓勵業者導入門禁系統監視攝影裝置等設備，並降低一般民眾對於業者分析、利用上述設備所蒐集資料之疑慮，以推動人工智慧等新技術應用於智慧化居住空間，內政部建築研究所委託資訊工業策進會科技法律研究所，參酌歐盟、日本等國家和地區有關促進監視攝影裝置資料利用之作法，編寫本問答集，提供各界參考。

貳、 名詞解釋

本問答集所使用之名詞定義如下；此處未提到之用語，原則上依我國《建築法》、《建築技術規則》、《個人資料保護法》等法規解釋。

一、智慧建築

根據內政部「智慧建築標章申請認可評定及使用作業要點」第 2 點，智慧建築係指『藉由導入資通訊系統及設備之手法，使空間具備主動感知之智慧化功能，以達到安全健康、便利舒適、節能永續目的之建築物。』另內政部建築研究所《智慧建築評估手冊》在序言中指出『智慧建築是應用網路、監測設備及系統整合等技術，讓建築物達到自動感知、分析及回應等功能，並在規劃設計之初，事先考慮使用者需求，提供需要的服務及後續維護管理的方便性，使建築物在完成之後，可以有最佳化之組合與運轉，以滿足使用者對安全、舒適、便利、效率的需求，並達到節能與降低維護管理人力經費之目標。』綜上所述，可知智慧建築是應用資通訊技術，使建築物可滿足使用者需求之建築物。

二、供公眾使用之建築物

根據《建築法》第 5 條，所謂供公眾使用之建築物，係指為供公眾工作、營業、居住、遊覽、娛樂及其他供公眾使用之建築物，參考台內營字第 0990801045 號令，其具體範圍如下：

1. 戲院、電影院、演藝場。
2. 舞廳（場）、歌廳、夜總會、俱樂部、加以區隔或包廂式觀光（視聽）理髮（理容）場所。
3. 酒家、酒吧、酒店、酒館。
4. 保齡球館、遊藝場、室內兒童樂園、室內溜冰場、室內游泳場、室內撞球場、體育館、說書場、育樂中心、視聽伴唱遊藝場所、錄影節目帶播映場所、健身中心、技擊館、總樓地板面積二百平方公尺以上之資訊休閒服務場所。
5. 旅館類、總樓地板面積在五百平方公尺以上之寄宿舍。
6. 總樓地板面積在五百平方公尺以上之市場、百貨商場、超級市場、休閒農場遊客休憩分區內之農產品與農村文物展示（售）及教育解說中心。
7. 總樓地板面積在三百平方公尺以上之餐廳、咖啡廳、茶室、食堂。

8. 公共浴室、三溫暖場所。
9. 博物館、美術館、資料館、圖書館、陳列館、水族館、集會堂(場)。
10. 寺廟、教堂（會）、宗祠（祠堂）。
11. 電影（電視）攝影廠（棚）。
12. 醫院、療養院、兒童及少年安置教養機構、老人福利機構之長期照護機構、安養機構(設於地面一層面積超過五百平方公尺或設於二層至五層之任一層面積超過三百平方公尺或設於六層以上之樓層者）、身心障礙福利機構、護理機構、住宿型精神復健機構。
13. 銀行、合作社、郵局、電信局營業所、電力公司營業所、自來水營業所、瓦斯公司營業所、證券交易場所。
14. 總樓地板面積在五百平方公尺以上之一般行政機關及公私團體辦公廳、農漁會營業所。
15. 總樓地板面積在三百平方公尺以上之倉庫、汽車庫、修車場。
16. 托兒所、幼稚園、小學、中學、大專院校、補習學校、供學童使用之補習班、課後托育中心、總樓地板面積在二百平方公尺以上之補習班及訓練班。
17. 都市計畫內使用電力（包括電熱）在三十七點五千瓦以上或其作業廠房之樓地板面積合計在二百平方公尺以上之工廠及休閒農場遊客休憩分區內總樓地板面積在二百平方公尺以上之自產農產品加工（釀造）廠、都市計畫外使用電力（包括電熱）在七十五千瓦以上或其作業廠房之樓地板面積合計在五百平方公尺以上之工廠及休閒農場遊客休憩分區內總樓地板面積在五百平方公尺以上之自產農產品加工（釀造）廠。
18. 車站、航空站、加油（氣）站。
19. 殯儀館、納骨堂（塔）。
20. 六層以上之集合住宅（公寓）。
21. 總樓地板面積在三百平方公尺以上之屠宰場。
22. 其他經中央主管建築機關指定者。

三、公共空間

根據《建築技術規則》第四章之一，設置安全維護裝置之公共空間包括：停車空間（室內/室外）、車道、車道出入口、機電設備空間出入口、電梯車廂內、安全梯間、屋突層機械室出入口、屋頂避難平台出入口、屋頂空中花園、公共廁所、室內公共通路走廊、基地內通路、排煙室、避難層門廳、避難層出入口。其中應設置監視攝影裝置之空間僅有停車空間（室內/室外）、車道、車道出入口和電梯車廂內，其餘空間視實際需求設置。

本問答集所指之公共空間，除應設置監視攝影裝置之空間外，亦包含其餘可視實際需求自由設置之空間在內。

四、門禁系統

建築物出入口進出管制措施，通常會利用刷卡、磁扣、指紋辨識、虹膜和人臉辨識等方式辨識來者身份，通過辨識者可進入管制區域。此外，社區內門禁系統常結合物業管理系統、中央監控系統或消防系統，以便發生火災或意外時能即時啟動消防通道和安全門，或透過系統直接通知中央監控室報警。

五、安全監控設備

建築物內安全監控設備分為設備監控和人員監控兩種，前者監視建築物內設備運轉狀況，後者則可進一步分為純影像拍攝、動態偵測和熱感應等類型。本問答集所稱之安全監控系統專指人員監控，亦即《建築技術規則》第四章之一「監視攝影裝置」。

六、個人資料

根據《個人資料保護法》第 2 條第 1 項第 1 款，個人資料為自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

七、資料主體

個人資料被蒐集、處理、利用之當事人。

八、資料蒐集、處理、利用主體

蒐集、處理、利用建築物內民眾個人資料之主體。

九、蒐集

根據《個人資料保護法》第 2 條第 1 項第 3 款，蒐集指以任何方式取得個人資料。

十、處理

根據《個人資料保護法》第 2 條第 1 項第 4 款，處理指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

十一、 利用

根據《個人資料保護法》第 2 條第 1 項 5 款，利用指將蒐集之個人資料為處理以外之使用。

參、 適用對象與範圍

（一） 適用對象

由於制定本問答集之目的，在於鼓勵業者於建築物內導入門禁系統或監視攝影裝置等設備，並降低一般民眾對分析、利用上述設備所蒐集資料之疑慮，以促進智慧建築資料之加值運用，讓資料可以用於完善建築物內各項服務，提升民眾生活品質，故**本問答集適用對象包括可能會被門禁系統及監視攝影裝置蒐集資料之一般民眾，以及擬於建築物內導入監視攝影裝置之建築物所有人、建商、建築師、設備廠商、保全業者、物業等相關從業人員**。

（二） 適用範圍

根據《建築技術規則》第四章之一「建築物安全維護設計」第 116 條之 1：「為強化及維護使用安全，供公眾使用建築物之公共空間應依本章規定設置各項安全維護裝置。」可知我國目前僅要求供公眾使用建築物之公共空間必須設置安全維護裝置，故本問答集適用範圍原則上以供公眾使用建築物之公共空間為主，並考量到部份非供公眾使用建築物，如小型商店、餐飲店等，仍有在公共空間裝設監視攝影裝置之需求，擬將其一併納入本問答集範圍，僅排除於建築物之私人空間，如個人於住家內外裝設監視攝影機，拍攝住家門口或周遭環境等情形。

此外，建築物內部份區域，如走廊，在訪談過程中亦發現有住戶希望管理單位能裝設監視攝影裝置，惟該區域雖非《建築技術規則》所列之公共空間，但亦非私人空間，使管理單位對於是否能裝設監視攝影裝置抱持疑問。為釐清上述疑問，本問答集亦擬針對在上述空間裝設監視攝影裝置相關問題進行整理。

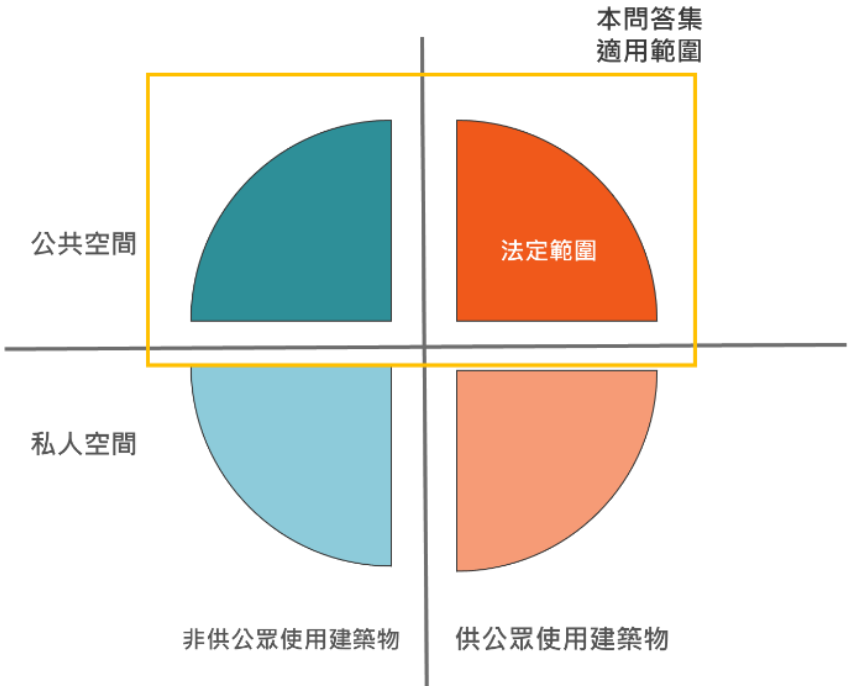


圖 1 本問答集適用範圍

資料來源：研究團隊自行繪製

傳統建築物內設置監視攝影裝置，通常係以人員監控為目的，而門禁系統則是為管控人員進出，惟在智慧建築發展趨勢下，建築物內裝設上述設備之目的不再僅限於監視或場域管理，可能還有統計人數、性別、年齡、人流動線等其他目的。本問答集經訪談及參考國外文獻後，整理建築物內導入前述裝置之情境、資料類型和用途如下表：

表 1 門禁系統應用情境和資料用途

	應用情境	資料類型	資料用途
門禁系統	在建築物出入口設置門禁，個人必須透過刷卡、指紋、虹膜、人臉辨識等方式進行驗證，進入特定區域	使用人姓名（持卡人）、職稱、住家電話、行動電話、地址、身分證字號、統一編號、戶別、車牌和車位、出入時間和進出次數、聲音等個人資料	4. 場域進出管理 5. 掌握特定人進出履歷、時間、動線，用於提供個人化服務

資料來源：研究團隊整理

表 2 監視攝影裝置運用情境和資料用途

	應用情境	資料類型	資料用途
監視攝影裝置	拍攝公共區域內影像	公共區域內特定或不特定多數人，以及周遭環境影像資料	9. 場域安全監控 10. 紀錄場域狀況 11. 統計人數 12. 統計性別和年齡等人物特徵 13. 紀錄人物座標和人流動線 14. 統計分析上述資料之間的關聯性 15. 將影像資料與其他資料進行比對 16. 利用影像資料訓練 AI 或進行產品研發

資料來源：研究團隊整理

綜上所述，**本問答集所適用之範圍，為裝設在公共空間之門禁系統和監視攝影裝置，且其裝設目的不僅限於場域進出管控或安全監控，包括蒐集、分析資料用於提供或優化各項服務在內**。在後續應用情境及案例分析中，本問答集將以上述資料用途為基礎，分別整理門禁系統和安全監控設備之應用情境。

肆、　門禁系統及安全監控設備資料應用之注意事項

一、門禁系統

（一）　門禁系統取得資料之特徵

目前部份辦公大樓、集合式住宅，或其他需要管制進出之區域，會透過刷卡、指紋、虹膜、人臉辨識等方式進行身份驗證，而為進行驗證，必須取得當事人資料，方能在系統中進行比對，允許符合資格者進入管制區域，故門禁系統通常會事先取得資料主體蒐集、處理、利用其個人資料之同意，以便將資料運用於場域進出管理。

門禁系統蒐集資料之目的，在於管理特定場域之進出狀況，而根據我國《個人資料保護法》第 5 條：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」故門禁系統所蒐集之資料，原則上不能用於場域進出管理以外之用途。

除事先蒐集資料用於身份驗證外，伴隨大數據及智慧化服務發展，資料主體通過門禁系統時所產生之資料，如進出時間、次數等，亦可進一步用於優化物業管理服務品質，如社區管理單位分析獨居高齡者每日進出大門時間和次數，當其長時間未出現或沒有依照往常時間進出時，物業便可前往關切，了解住戶是否發生需要協助的狀況。有鑑於此，為促進門禁系統所蒐集資料之應用，在事先取得資料主體蒐集、處理、利用資料同意時，還需讓其了解門禁系統會保留進出紀錄，而這些看似無用的資料，未來可能有其他用途。

另外，建築物時常會有訪客出入，門禁系統可能也會需要蒐集訪客資料，除掌握訪客身份及管控其進出外，亦可透過知道訪客在幾點幾分通過門禁系統，從而推算出訪客會在什麼時候抵達目的地，以便安排人力在該地點等待。由於訪客只能在進出場域當下才能告知並取得蒐集、處理、利用其個人資料之同意，故該如何落實《個人資料保護法》之告知義務，以及取得資料主體同意，且確保所取得之資料不會逾越比例原則之限制，成為需要注意的

問題。

（二） 門禁系統資料應用流程

從上述說明，可知門禁系統在取得資料時，通常分為兩種途徑：事先告知並取得資料主體同意，以及當場告知並取得資料主體同意，惟無論是事先告知或當場告知，都是在蒐集前取得當事人同意，在處理流程上並無太大差異。在門禁系統資料從蒐集到利用之過程中，真正會產生差異之處，應僅在於蒐集資料的方式和後續之資料用途。本問答集根據前述門禁系統之應用情境、資料類型和資料用途，整理門禁系統資料應用流程如下：

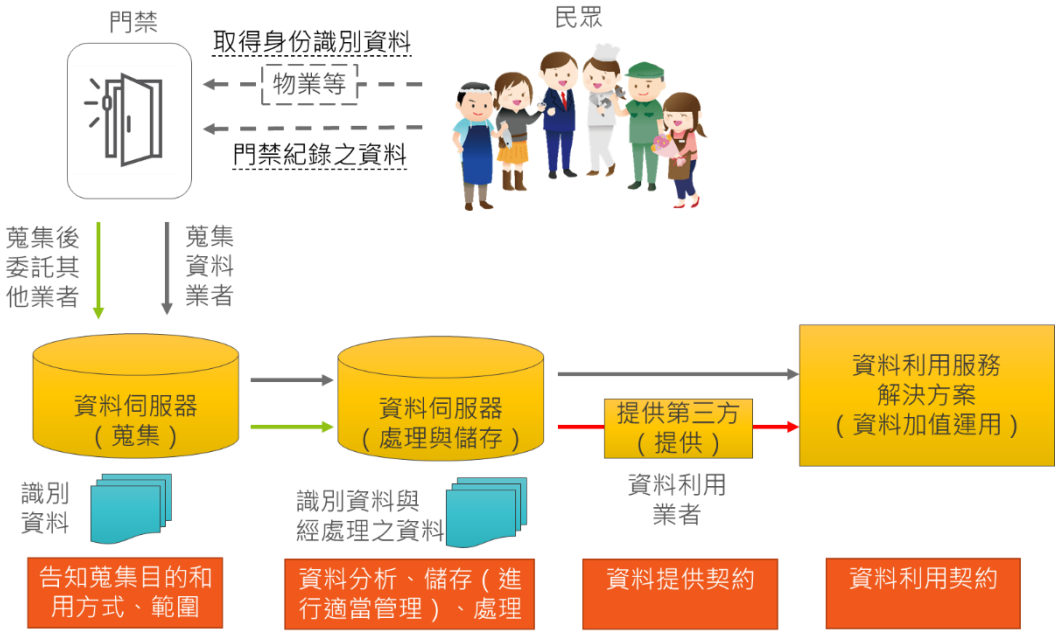


圖 2 門禁系統之資料應用流程

資料來源：研究團隊自行繪製

二、監視攝影裝置

（一） 監視攝影裝置取得資料之特徵

根據《建築技術規則》第四章之一「建築物安全維護設計」，供公眾使用建築物之公共區域應設置安全維護裝置，而監視攝影裝置即為其中一種。除上述區域外，因應社區大樓內住戶或建築物使

用者之需求，監視攝影裝置可能還會設置在其他區域，且用途並不僅限於安全監控，惟無論如何，由於監視攝影裝置本身具有設置地點隱密、不易被發現，事先很難取得資料主體同意等特性，故其取得資料時往往具備以下特徵：

- 根據拍攝範圍之設定及週邊環境影響，監視攝影裝置可能會拍到玻璃或鏡面中之反射影像，或經過建築物附近的路人，被拍攝之資料主體不一定知道自己會被拍攝，拍攝者也無法一一告知或取得被拍攝人同意。
- 對於被拍攝之資料主體而言，無法僅從監視攝影裝置外觀得知其設置之目的，以及所拍攝之影像資料將如何被運用。
- 監視攝影裝置可以紀錄資料主體的一舉一動，以及周遭環境變化，影像內存有龐大的資訊量，其中所透露之訊息可能已經逾越資料主體願意被蒐集的範圍，或資料主體根本沒有意識到可能會被蒐集。
- 伴隨技術進步，影像資料經進一步分析後，原先無意義的影像都有可能存在利用價值。

（二） 監視攝影裝置之資料應用流程

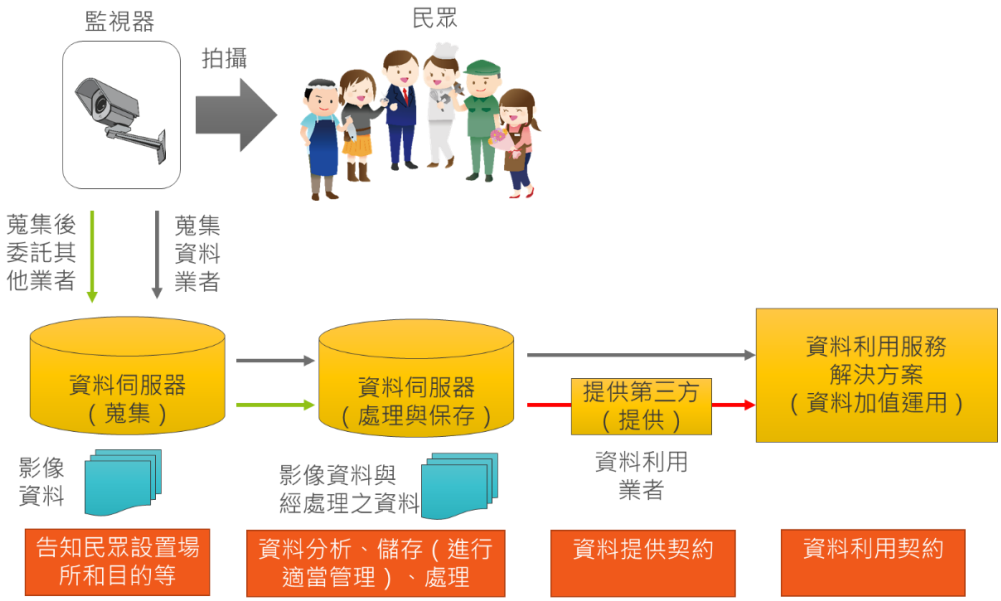


圖 3 監視攝影裝置之資料應用流程

資料來源：研究團隊自行繪製

一、資料應用流程中各階段之注意事項

從上述資料應用流程，可發現門禁系統和監視攝影裝置資料在應用上，大致可分為蒐集、處理、利用三個階段，惟在進入上述階段前，尚須確認系爭資料是否為個人資料，以及資料類型等問題，方能確定在後續流程中應遵守哪些規定，故本問答集將參考我國《個人資料保護法》規範架構，依序整理上述資料應用階段需注意的問題，並針對各階段之注意事項提出建議。

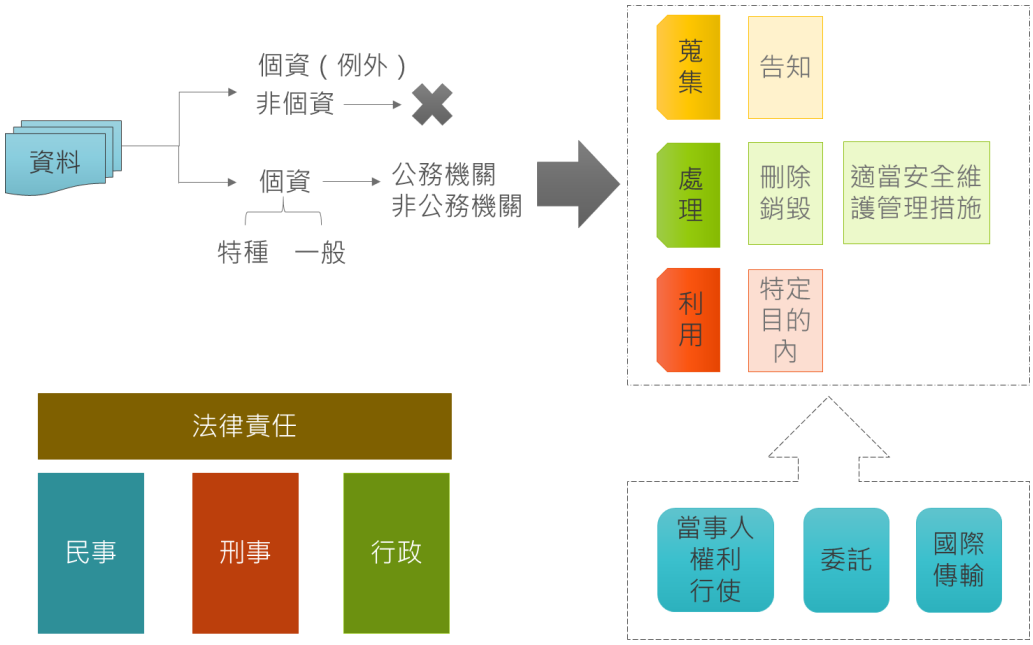


圖 4 我國《個人資料保護法》之規範架構

資料來源：研究團隊自行繪製

（一） 判斷是否為個人資料

我國《個人資料保護法》第 2 條第 1 項規定，個人資料指『自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。』上述規定前段為例示規定，立法者以列舉方式，告訴民眾哪些資料為個人資料，而後段則直接表示「其他得以直接或間接方式識別該個人之資料」為個

人資料，故只要符合後段定義者，縱使沒有列在前段，亦為我國《個人資料保護法》所稱之個人資料。

由於只要「得以直接或間接方式識別該個人之資料」均為個人資料，故如何判斷系爭資料為個人資料，成為資料應用之重要前提。針對某些資料是否為個人資料，本問答集將綜整訪談過程中所蒐集到之問題，以 Q&A 形式加以說明：

Q1 姓名、員工號碼、職稱、住家電話、行動電話、地址、身分證字號、統一編號、戶別、車牌和車位、聲音等.....門禁系統用來辨識身分之資料，是否為個人資料？

智慧建築內之門禁系統，為辨識特定人身份，可能會需要蒐集姓名、員工號碼、職稱、住家電話、行動電話、地址、身分證字號、統一編號、戶別、車牌和車位、聲音等資料，上述資料因可直接或間接辨識出特定個人，故均該當我國法上之個人資料，在後續蒐集、處理及利用過程中，必須遵守我國《個人資料保護法》之規定。

門禁系統會紀錄民眾進出時間和次數等資訊，這些紀錄可以呈現特定個人日常生活的行動軌跡，與其他資料結合後亦有可能辨識出特定各人，故亦有該當個人資料之可能。有鑑於此，門禁系統在取得及利用上述資料時，亦須注意《個人資料保護法》之規定。

Q2 個人通過門禁系統之時間、次數等紀錄，是否為個人資料？

惟單純紀錄進出次數之計數資料，如圖書館統計當日或當月入館人數，由於無法識別出特定個人，故非個人資料。

Q3 設置在公共區域之監視攝影裝置，如果只有拍攝建築物等風景，沒有拍攝到民眾，則是否仍為個人資料？

如果影像資料內沒有任何人，則非個人資料，無《個人資料保護法》之適用。

Q4 設置在公共區域之監視攝影裝置，如拍攝不特定之多數人影像（如設置在車站之監視器，每天都會拍到大量往來民眾），這些

雖然監視攝影裝置拍攝到大量民眾影像，但這些影像所拍攝之對象為不特定多數人，無法知道誰會被拍攝到，如果又難以從影像中辨識出特定個人，則此種資料應非個人資料，不適用《個人資料保護法》。必須注意的是，假使能從影像中辨識出特定個人，如監視攝影裝置清楚地拍攝到人群中某人的臉部或身體特徵，與其他資料比對後可以知道對方是誰，則該影像資料仍有可能是個人資料。

參考資料：

法務部法律字第 0999009760 號函釋：「內政部警政署提案修正「金融機構安全維護管理辦法」第 5 條之規定，擬將金融機構「營業處所前道路」納入攝錄範圍，其取得之資料須為建立個人資料檔案而取得足資識別該個人之影像資料，予以電腦處理者，始有電腦處理個人資料保護法之適用；反之，若尚無建立個人資料檔案，且**僅錄存不特定自然人影像而未予識別該個人以前，相關監視錄影系統之設置管理問題，則應無該法之適用**。」

Q5 設置在公共區域之監視攝影裝置，如拍攝特定多數人之影像（如設置在集合式住宅內之監視器，原則上只會拍攝到社區住戶和

此種狀況與前者類似，然而雖然同樣會拍攝到許多人，惟因可以特定出被拍攝人之身份，故在此種狀況下所拍攝之影像資料有該當個人資料之可能。以問題中設置在集合式住宅內之監視攝影裝置為例，被拍攝人可能為住戶或訪客，前者每天都會出入集合式住宅，經比對住戶資料後就可確認身份，故為個人資料；而後者如果無法經由其他資料（如物業登記之訪客資料）比對後確認身份，則仍非個人資料。

Q6 設置在公共區域之監視攝影裝置，如拍攝特定人之影像，該資料是否為個人資料？

監視攝影裝置所拍攝之影像，如拍攝到足以識別出特定個人之影像，無論是拍到當事人正面或鏡面、玻璃窗中反射影像，均為個人資料，需要依照《個人資料保護法》規定蒐集、處理、利用。

Q7 擷取臉部影像或身體影像特徵之資料，如臉上的疤痕、走路姿勢、體型等，是否為個人資料？根據特徵資料分析出之人物屬性，如具有某些特徵之人通常為男性或女性等，是否為個人資

《個人資料保護法》第 2 條第 1 項規定，個人資料指『自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、**特徵**、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。』上述條文中明確指出「特徵」為個人資料，故這些資料雖然可能無法直接用以識別特定個人，但仍為個人資料。

如果進一步分析特徵資料，從而歸納出某些性別、年齡或體型的人可能會具備之特徵，則這些經分析、歸納出之人物屬性資料，如果沒有辦法回溯到特定個人身上，則非個人資料。如擷取十位兒童全身影像，蒐集到每位兒童身高、胖瘦等體型特徵，這些特徵資料為個人資料；惟如進一步分析上述特徵資料，得知十位兒童平均身高和體重，則平均身高和體重數字無法和特定兒童連結在一起，故該平均身高和體重資料並非個人資料。

Q8 監視攝影裝置拍攝到之人物動線資料是否為個人資料？如果進一步將動線資料轉化為座標值，則該資料是否為個人資料？

人物動線資料為特定個人之行動履歷，可直接或間接識別出該個人，故為個人資料。惟如進一步分析動線資料，將其轉

化座標值，如 2 點 50 分（255，370），則除非該座標值會與其他資料串連比對，否則應無法僅從數字識別出該個人，故非個人資料。

Q9 什麼是一般資料和特種資料？門禁系統和監視攝影裝置所取得之資料是一般資料還是特種資料？

《個人資料保護法》第 6 條第 1 項規定：「有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。」上述列在條文中之個人資料即為特種資料，除符合例外情形，原則上不得蒐集、處理和利用，而非屬上述資料之個人資料即為一般資料，只要遵守《個人資料保護法》之規定，就可蒐集、處理和利用。

門禁系統所取得之資料，以及監視攝影裝置所拍攝之影像，只要不屬於上面所列之資料，即非特種資料。

Q10 哪些個人資料不適用《個人資料保護法》？現在常聽到之去識別化資料又是什麼意思？

《個人資料保護法》第 2 條第 1 項規定，個人資料指『**自然人**之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他**得以直接或間接方式識別該個人**之資料。』由此可知，只有得以識別該個人之自然人資料才是個人資料。換言之，非自然人，如往生者，或無法識別該個人之資料均不適用《個人資料保護法》。

此外，《個人資料保護法》第 51 條第 1 項規定：「有下列情形之一者，不適用本法規定：一、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。」故個人為舉辦同學會蒐集同學聯絡資料，或公司活動中所拍攝之尚未與其他資料結合之影片和照片，亦不適用《個人資料保護法》。

最後，所謂去識別化資料係指經處理後無法識別特定個人之

資料。惟我國《個人資料保護法》並未明文定義去識別化以及去識別化方式，故有關去識別化標準，必須參考經濟部標準檢驗局於 2014 年 6 月和 2015 年 6 月公布之國家標準 CNS29100「資訊技術-安全技術-隱私權框架」，以及 CNS29191「資訊技術-安全技術-部分匿名及部份去連結鑑別之要求事項」。此外，經濟部標準檢驗局亦於 2019 年 2 月 20 日公布「資訊技術-安全技術-個人可識別資訊保護之作業規範」、「資訊技術-安全技術-個人可識別資訊去識別化過程管理系統-要求事項」草案，擬將個人資料去識別化處理之業者，可參考上述文件為之。

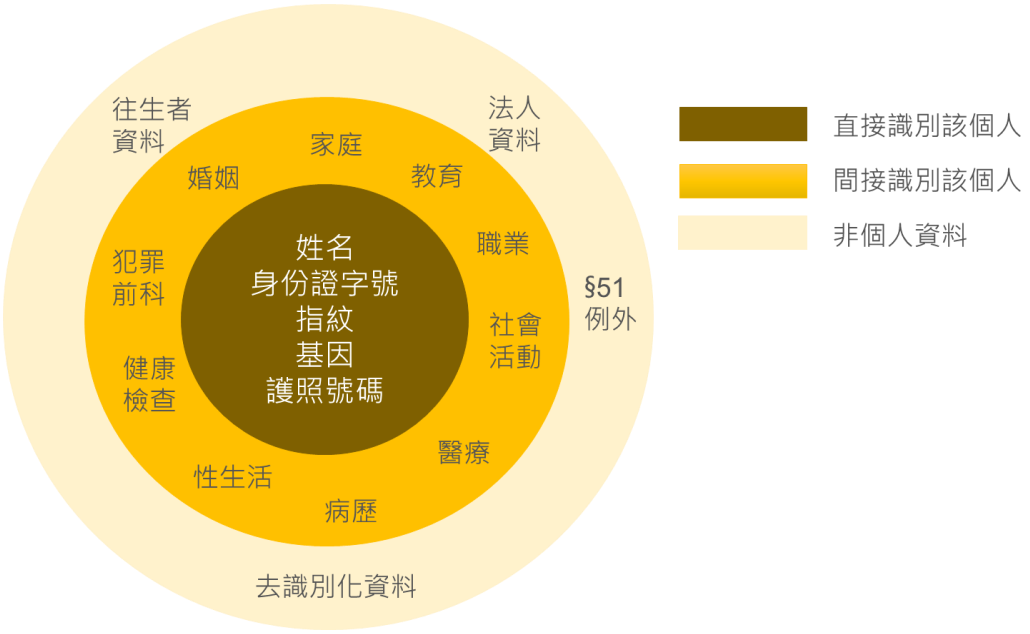


圖 5 我國《個人資料保護法》之適用範圍

資料來源：研究團隊自行繪製

（二） 資料蒐集

在釐清系爭資料是否為個人資料，以及資料類型（一般資料或特種個資）等問題後，接下來要討論的問題是在資料應用流程（蒐集、處理、利用）各階段分別有哪些注意事項。首先，在最初的

資料蒐集階段，《個人資料保護法》第 8 條[77]及第 9 條[78]規定，在蒐集當事人資料前，除符合特定情形外，應向其告知（1）蒐集單位名稱（2）蒐集目的（3）蒐集之個人資料類別（4）個人資料利用之期間、地區、對象及方式（5）根據同法第 3 條[79]，當事人可以請求閱覽、補充、更正、停止蒐集、處理或利用、刪除等（6）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.....等事項。基於上述理由，無論係透過門禁系統或監視攝影裝置取得當事人資料，理論上都應遵守個資法規定，向當事人告知應告知事項。

然而，要徹底落實上述規定並不容易，以門禁系統為例，如係事先針對住戶或員工等蒐集資料，自然可以清楚地告知當事人蒐集

---

77 《個人資料保護法》第 8 條：「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。有下列情形之一者，得免為前項之告知：一、依法律規定得免告知。二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。三、告知將妨害公務機關執行法定職務。四、告知將妨害公共利益。五、當事人明知應告知之內容。六、個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。」

78 《個人資料保護法》第 9 條：「公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。有下列情形之一者，得免為前項之告知：一、有前條第二項所列各款情形之一。二、當事人自行公開或其他已合法公開之個人資料。三、不能向當事人或其法定代理人為告知。四、基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。第一項之告知，得於首次對當事人為利用時併同為之。」

79 《個人資料保護法》第 3 條：「當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：一、查詢或請求閱覽。二、請求製給複製本。三、請求補充或更正。四、請求停止蒐集、處理或利用。五、請求刪除。」

資料之目的、蒐集的資料類別、利用期間等.....事項，但如果是針對訪客當場進行告知，則恐怕難以清楚地向當事人說明或讓當事人理解告知的內容。如此一來，後續就有可能因雙方認知上的誤差而產生爭議。

再以監視攝影裝置為例，前面提到監視攝影裝置可能因為設置地點較隱密、拍攝範圍較廣，或可能拍攝到不特定多數人等原因，使得在拍攝時很難告知當事人。即便透過張貼告示等方式，向被拍攝人告知正在蒐集其影像資料，也無法確保所有人都會仔細閱讀告示或理解告示內容，故對欲導入相關設備之業者而言，該如何落實《個人資料保護法》有關告知義務之規定，成為急需解決的重要問題。針對告知內容及方式，本問答集將綜整訪談過程中所蒐集到之問題，以 Q&A 形式加以說明：

Q11 關於蒐集個人資料前要告知當事人之規定有無例外？例外分別是哪些情形？如果門禁系統蒐集資料目的只是為驗證身份，或用於改善管理服務，是否不用告知當事人？

根據《個人資料保護法》第 8 條第 2 項規定，有 6 種例外情況可以免除告知義務：（1）依法律規定得免告知（2）公務機關為執行法定職務，或非公務機關為履行法定義務而蒐集資料（3）告知將妨害公務機關執行法定職務（4）告知將妨害公共利益（5）當事人明知應告知之內容（6）個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

如果門禁系統蒐集當事人資料只是為驗證其身份，或用以改善管理服務品質，並非出於營利考量，且對當事人無不利影響，則蒐集時應不用告知當事人。

參考資料：

法務部法律字第 10503503290 號函釋：「本件貴府擬建置公務線上通訊錄，資料包括貴府所有人員及所屬機關學校之一級主管人員之服務機關、單位、科別、職稱、姓名、公務電話及公務電子信箱等，以供所屬人員公務上查詢使用，可認**係貴府基於人事管理（特定目的代號 002）或公務聯繫業務推動（特定目的代號 175 等）之目的，而於執行法定職務之必要範圍內，所為個人資料之蒐集、處理及利用行為**，揆諸上

開規定，無須再經當事人書面同意。」

法務部法律字第 10403513100 號函釋：「查本件所詢涉及違反不動產經紀業管理條例之行政罰裁處，行政機關為調查事實及證據，所採取之調查方法是否違法等節，參酌前揭說明，**貴局以隱藏式攝影、錄音器材蒐集得識別特定個人之影音資料，如係基於執行法定職務必要範圍內而蒐集、處理、利用個人資料，即得免踐行告知義務，尚無違反個人資料保護法之問題**。」

法務部法律字第 10203510680 號函釋：「按個資法第 8 條第 2 項第 2 款規定所稱「非公務機關履行『法定義務』所必要」，**僅限於行政法上義務，不包括民法上之義務**。」

法務部法律字第 10100699790 號函釋：「按個資法第 8 條第 2 項第 1 款及第 19 條第 1 項第 1 款所稱「法律」，**指法律或法律具體明確授權之法規命令**（個資法施行細則第 9 條參照）。又個資法第 8 條第 2 項第 2 款所稱「法定義務」，**係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**。」

Q12 如果監視攝影裝置設置目的只是為監控場域安全，是否不用特別告知當事人？目前一般大樓或商場內都有設置監視器，理論上是要底片都對此有所認識，是否符合不用告知的例外？

如果監視攝影裝置只是單純拍攝場域內影像，並非出於營利目的且對當事人無不利影響，則亦符合不用告知之例外。必須注意的是，雖然目前大樓或商場、停車場等地方通常都設有監視攝影裝置，民眾也知道會被拍攝，但僅從監視攝影裝置外觀及設置地點，無法知道是哪個單位在蒐集資料，也無從得知蒐集影像之目的、期間和用途等應告知內容，故恐怕無法以當事人明知告知內容為由，主張不用告知當事人。

Q13 如果蒐集之資料不是由當事人直接提供（業者只是間接取得），是否還需告知當事人？門禁系統和監視攝影裝置可能有間接取得資料的狀況發生嗎？

假使資料不是由當事人提供，如蒐集當事人已經公開在網路上的電子郵件、公司電話等資料，根據《個人資料保護法》第 9 條第 1 項規定，在蒐集時不用告知當事人，直到要處理和利用資料時，才需要向當事人告知。此外，與直接蒐集當事人資料不同，在間接蒐集資料的狀況下，蒐集時還需向當事人說明資料來源。

《個人資料保護法》第 9 條第 2 項亦設有例外規定，除符合第 8 條第 2 項所列情形外，如果是（1）當事人自行公開或其他已合法公開之個人資料（2）不能向當事人或其法定代理人為告知（3）基於公共利益為統計或學術研究之目的而蒐集，且該資料經提供者處理後或蒐集者依其揭露方式，已無從識別特定當事人（4）大眾傳播業者基於新聞報導之公益目的而蒐集.....等情形，亦可免於向當事人為告知。

依照門禁系統和監視攝影裝置之運作方式，兩者直接蒐集當事人資料，理論上不太可能發生間接取得個人資料的問題。

參考資料：

法務部法律字第 10303511680 號函釋：「蒐集資料者所蒐集之**個人資料如屬已依法公示、公告或以其他合法方式公開者（如政府資訊公開法第 7 條應公開之政府資訊），因該等人之個人隱私應無被侵害之虞（第 9 條、第 16 條之立法理由參照），則其蒐集符合個資法第 19 條規定，且免為個資法第 9 條所定告知義務**。」

Q14 在沒有辦法當面告知當事人，卻又不符合例外規定的狀況下，如商店在室內設置監視攝影裝置拍攝人流影像，作為日後改善結帳動線之資料時，店家該如何履行《個人資料保護法》有關

如果沒有辦法當面告知當事人，或許可以考慮透過張貼告示等方式為之，讓當事人知道自己正在被蒐集資料。關於張貼方式、地點和內容，本問答集將於「伍、門禁系統及監視攝影裝置之資料應用情境」，透過情境式描述加以說明。

蒐集個人資料除須告知當事人外，還應具有特定目的，換言

Q15 《個人資料保護法》規定蒐集、處理、利用個人資料需有特定目的或符合特定情形，特定目的和特定情形是指什麼？門禁系統或監視攝影裝置蒐集資料可能符合哪些特定目的、另外，告

之，不能毫無理由就隨便蒐集個人資料。關於蒐集個人資料之目的，必須在蒐集時一併告知當事人，同時需要說明所蒐集資料之類別。

關於蒐集資料之特定目的，以及個人資料之類別，可以參考附件「法務部個人資料保護法之特定目的及個人資料之類別」。至於公務機關和非公務機關蒐集資料所應符合之特定情形，則分別規定於《個人資料保護法》第 15 條及第 19 條。

門禁系統或監視攝影裝置蒐集資料，可能適用之特定目的包括：（○○七）不動產服務；(○六九）契約、類似契約或其他法律關係事務；(○七一）建築管理、都市更新、國民住宅事務；(一一六）場所進出安全管理；(一六四）營建業之行政管理；(一七六）其他自然人基於正當性目的所進行個人資料之蒐集處理及利用.....等。

此外，《個人資料保護法》亦規定個人資料之「蒐集和處理」必須符合特定情形，且根據蒐集單位是公務機關或非公務機關會有所不同。有關特定情形之問題，將一併在處理階段加以說明。

參考資料：

法務部法律字第 10403505690 號函釋：「本件警察機關基於「行政裁罰、行政調查」(代號 039）之特定目的，於執行道路交通管理處罰條例第 7 條之 1、第 7 條之 2 規定之法定職務時，因須調查受舉發人之違規事實，爰蒐集違規行為、違規現場之照片，其內雖含有其他非受舉發人（乘客）之影像，**若影像清晰且與其他資料對照、組合、連結後具間接識別可能者，固仍屬個資法所稱個人資料，惟為維持該採證照片之真實性、完整性，其蒐集認屬與執行法定職務有關之必要範圍內，仍符合個資法第 15 條規定。**至於該等個人資料之利用，即**舉發單併同前揭採證照片送達被通知人，係為證明違規事實及違規當時之客觀情狀，應與警察機關蒐集之特定目的相符，且屬執行上開法定職務必要範圍內，符合個資法第 16 條規定**。」

（三） 資料處理

根據《個人資料保護法》第 15 條規定，**公務機關**蒐集、處理資料時必須具有特定目的，並符合（1）執行法定職務必要範圍內（2）經當事人同意（3）對當事人權益無侵害等情形；另根據《個人資料保護法》第 19 條，**非公務機關**蒐集資料時，則應符合（1）法律明文規定（2）與當事人有契約或類似契約之關係，且已採取適當之安全措施（3）當事人自行公開或其他已合法公開之個人資料（4）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經蒐集者依其揭露方式無從識別特定之當事人（5）經當事人同意（6）為增進公共利益所必要（7）個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限（8）對當事人權益無侵害等情形。

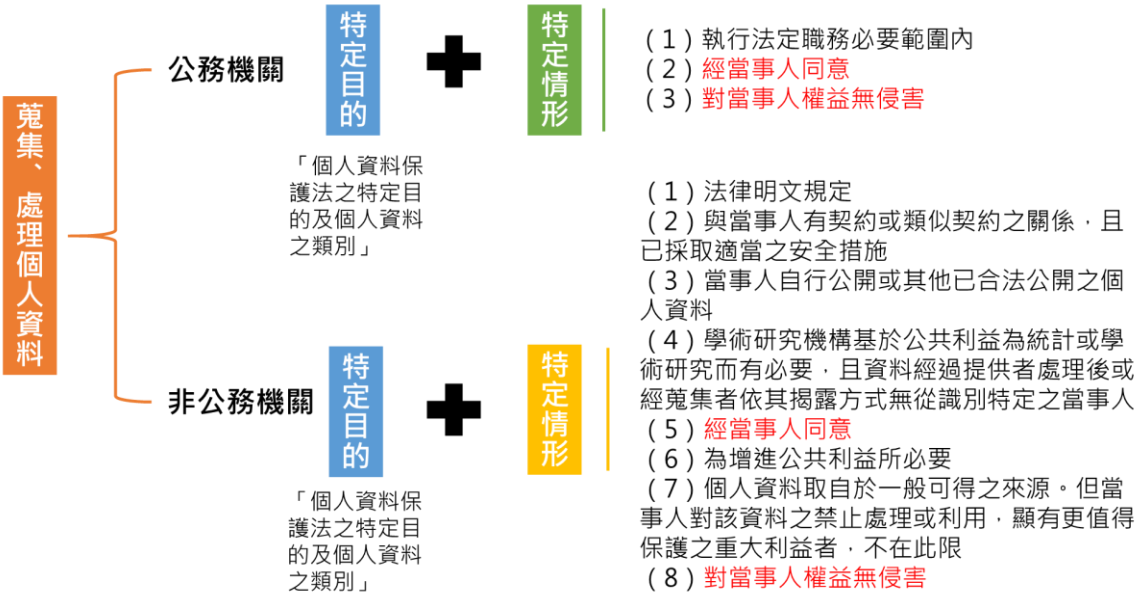


圖 6 蒐集、處理個人資料之特定目的和特定情形

資料來源：研究團隊自行繪製

從上述圖示，可知蒐集、處理個人資料應符合哪些情形。必須注意的是，縱使蒐集、處理個人資料時不符合法定情形，但只要有取得當事人同意，或對當事人權益無侵害，仍然可以蒐集、處理個人資料。

Q16 什麼樣的行為是「處理」個人資料？將監視攝影裝置或門禁系統所蒐集之個人資料編號後儲存在資料庫之行為，也是「處理」個人資料嗎？

所謂個人資料之處理，係指『為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送』等行為，而前述之個人資料檔案，則是指『依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。』

監視攝影裝置所拍攝之影像，門禁系統所蒐集之個人資料，如係為建立或利用個人資料檔案而儲存於資料庫內，都是處理個人資料之行為。

參考資料：

法務部法律字第 10103104550 號：「以錄音裝置蒐集個人資料者，**必先係為建立得以自動化機器或其他非自動化方式檢索、整理之個人聲音資料集合，而後取得足資直接或間接識別該個人之影音資料時，方屬個資法之蒐集行為**；換言之，**取得之個人資料須足資識別該個人者，始適用個資法**。……本件貴公司客服人員與客戶間於客服專線有關核對用戶基本資料等通話內容，進行全程錄音存檔乙節，如其聲音資料未經識別為特定自然人前，尚無個資法之適用問題。若電話錄音內容得直接或間接識別特定個人者，涉屬「足資識別該個人之資料」，其蒐集、處理或利用，除法律另有規定外，即受個人資料保護法之規範。」

Q17

關於當事人表示同意之方式，《個人資料保護法》是否有所規定？如果當事人僅口頭表示允許是否合法？如果當事人沒有表示同意，但亦沒有明確表示拒絕，是否可以推定其同意蒐

關於表示同意之方式，《個人資料保護法》針對蒐集、處理和利用有不同的規定。針對蒐集和處理，當事人只要有表示出允許之意思即可，就算不是非常明確的表示，只有點頭示意亦可。此外，雖然當事人什麼都沒講，但如果沒有明確表示反對並已提供個人資料，也可認為其同意我們蒐集、處理其個人資料。惟利用的狀況不同，要利用個人資料必須取得當

事人明確的表示,不能只以當事人有點頭或沒表示反對為由，就認為對方已經同意我們利用其個人資料。

在取得當事人同意時，原則上不以書面為限，只要當事人在被告知相關事項後表示同意即可。然而病歷、醫療、基因、性生活、健康檢查及犯罪前科等特種資料之蒐集、處理和利用，就必須以書面取得當事人同意，且不能以當事人未表示反對為由，推定其已經同意，與一般資料不同。

（四） 資料利用

近年因人工智慧和大數據等技術和議題影響，如何利用資料並讓資料發揮最大價值，成為輿論所關注之焦點。由於《個人資料保護法》規定，原則上利用個人資料須符合蒐集時之特定目的，故必須注意如何在遵守《個人資料保護法》前提下善加運用資料，發揮資料價值。

Q18 什麼樣的行為是「利用」個人資料？利用個人資料時有哪些需要注意的地方？

所謂利用個人資料，係指處理個人資料以外之使用，如分析個人資料或將個人資料用於電話行銷等。在利用個人資料時，如利用者為公務機關，利用之行為應於執行法定職務必要範圍內為之，並與蒐集時之特定目的相符；如利用者為非公務機關，則只要利用個人資料符合蒐集時之特定目的即可。

參考資料：

法務部法律字第 10503520020 號：「上開規定所稱「法定職務」**係指於法律、法律授權之命令所定公務機關之職務**（個資法施行細則第 10 條第 1 款參照）。是以，貴會基於特定目的（例如：電信及傳播監理，代號：144），於執行電信法及船舶無線電臺管理辦法（下稱管理辦法）相關規定所定管理

船舶無線電臺（含 EPIRB 設備）之法定職務必要範圍內，蒐集電臺執照持有者之相關個人資料（管理辦法第 19 條規定參照），符合上開個資法第 15 條第 1 款規定。又貴會蒐集上開管理辦法第 19 條規定申請書應填具及檢附之相關個人資料以外，有關「EPIRB 資訊（如 15 個字元識別碼）及持有者緊急聯絡人」等資料，**如不在前開貴會辦理船舶無線電臺管理及核照之法定職務範圍內，即不得以個資法第 15 條第 1 款規定為依據蒐集上開個人資料**。」

法務部法律字第 10303511680 號：「倘資訊業者僅研發軟體工具供使用者即個人資料之蒐集者，於資料蒐集後之編輯、建置地籍資料之用，**資訊業者本身並無蒐集個人資料者，自與個資法無涉**。」

Q19

如果監視攝影裝置一開始蒐集個人資料是為監控場域安全，後來才想進一步分析所蒐集之資料，如統計人數和分析動線，是否可能因不符合原先蒐集之目的，而違反《個人資料保護法》規定？在什麼情況下，即便不符合特定目的，仍然可以利用個

由於《個人資料保護法》要求利用個人資料須符合蒐集時之目的，故利用者不能隨便將蒐集來的個人資料拿去做其他用途。不過為促進個人資料之利用，《個人資料保護法》第 16 條和第 20 條，分別針對公務機關和非公務機關設有例外規定，清楚列出在符合哪些條件狀況下，可以為特定目的外之利用：

《個人資料保護法》第 16 條（針對公務機關）所規定之例外情況：（1）法律明文規定（2）**為維護國家安全**或增進公共利益所必要（3）為免除當事人之生命、身體、自由或財產上之危險（4）為防止他人權益之重大危害（5）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經蒐集者依其揭露方式無從識別特定之當事人（6）有利於當事人權益（7）經當事人同意。

《個人資料保護法》第 20 條（針對非公務機關）所規定之例外情況：（1）法律明文規定（2）為增進公共利益所必要（3）為免除當事人之生命、身體、自由或財產上之危險（4）為防止他人權益之重大危害（5）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經蒐集者依其揭露方式無從識別特定之當事人（6）有利於當事人權益（7）經當事人同意。

綜觀上述規定，除公共機關可基於維護國家安全利用個人資料外，其餘規定大致相同，且就算都不符合例外狀況，只要取得當事人同意，仍然可以利用其個人資料。

參考資料：

法務部法律字第 10503518090 號：「次按個人資料保護法第 16 條但書第 7 款規定：**「經當事人同意」，僅是個人資料於特定目的外利用要件之一**，雖能達到避免人格權侵害之方法，惟**若同時具有個人資料保護法第 16 條但書第 1 款至第 6 款等其他個人資料之合理利用事由者**（例如：「增進公共利益所必要」、「為免除當事人之生命、身體、自由或財產上之危險」、「為防止他人權益之重大危害」等），**公務機關基於比例原則與具體情況，仍可於特定目的外利用個人資料，以求法益平衡，並非一律均需取得當事人同意**。」

法務部法律字第 10503512050 號：「而警察機關將臨檢紀錄表之個人資料與所屬員警資料庫進行比對，則屬特定目的外之利用行為，倘如貴署來函所稱能先期掌握違紀員警加強督導考核，達成「整飭官箴、杜絕貪腐」之目的，雖可認為符合個資法第 16 條但書第 2 款「增進公共利益所必要」之規定，而得為特定目的外利用，惟查，**個人資料之利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，個資法第 5 條定有明文，是個人資料之利用，除應符合個資法第 16 條之利用規定，並應符合個資法第 5 條比例原則之規定**。準此，警察機關為查察員警風紀狀況，避免所屬員警有違紀案件發生，而將經列管之不妥當場所之所有受臨檢民眾之個人資料與所屬員警資料庫進行比對，此種全部、通案、預先之比對機制，恐有違反比例原則之虞，建請貴署審慎再酌。」

Q20 如當事人表示同意，就可以在特定目的範圍外利用該個人資料，此時的「同意」與當事人同意蒐集、處理個人資料，兩者有何不同？

根據《個人資料保護法》第 7 條第 2 項規定，在利用當事人個人資料時需要取得之同意，係指經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示。換言之，當事人必須明確表示同意，不能只以肢體動作（如點頭）就認為當事人已表示同意，或主張當事人沒有明確表示拒絕，故推測其已表示同意。

綜上所述，如果門禁系統或監視攝影裝置只是單純蒐集、處理個人資料，則只要在告知當事人後，當事人有點頭或沒有明確拒絕並提供資料，就可以認為當事人同意我們蒐集、處理其個人資料；但如果要進一步利用所蒐集之個人資料，就需要得到當事人明確的回覆。此外，如果所蒐集到之資料為特種個資，就需要取得當事人書面同意。

Q21 在利用個人資料時，還有哪些需要特別之注意規定？

《個人資料保護法》第 20 條第 2 項和第 3 項規定，如果非公務機關想將所蒐集之資料用於行銷，則當事人表示拒絕時，應立即停止利用其個人資料行銷；且於首次行銷時，必須告訴當事人拒絕接受行銷之方式，並支付所需費用。換言之，無論蒐集資料時是否有告知當事人蒐集目的包括行銷，抑或行銷符合特定目的外利用之情形，當事人都可以主動表示拒絕行銷。

參考資料：

法務部法律字第 10503501900 號：「非公務機關利用個人資料從事商品行銷時，**無論係特定目的內或特定目的外之利用，本法賦予當事人拒絕接受行銷之權利，以保障其免受行銷之打擾；當事人表達拒絕接受行銷之意思表示時，非公務機關應即停止再利用其個人資料進行行銷，爾後亦不得再利用其**

個人資料進行行銷。倘非公務機關違反「應即停止利用其個人資料行銷」之義務，其法律效果係由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣 2 萬元以上 20 萬元以下罰鍰（本法第 48 條第 3 款參照）。」

Q22 如建築物所有人或業者係委託他人蒐集、處理、利用個人資料，需要注意哪些事情？

《個人資料保護法》第 4 條規定：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」故受他人委託蒐集、處理或利用個人資料者，仍須遵守《個人資料保護法》相關規定。如果受委託業者為民間單位，但委託者為公務機關，則受委託業者應適用有關公務機關之規定。

另外，《個人資料保護法施行細則》第 8 條規定，委託他人蒐集、處理或利用個人資料，應對受託者為適當之監督，且須定期確認受託者執行狀況。其監督事項至少應包含：（1）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（2）受託者就第十二條第二項採取之措施（3）有複委託者，其約定之受託者（4）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（5）委託機關如對受託者有保留指示者，其保留指示之事項（6）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。

附錄十五：問答集草案第二版

一、前言

伴隨時代進步，物聯網、大數據、人工智慧等新技術開始應用於建築物，衍生許多創新應用服務。智慧化居住空間之創新應用，例如智慧門禁系統、安全監控系統、健康照護，空調、照明、電梯等設備之節能管理等，可透過聯網設備或感測器蒐集個人生理及日常活動資料，用於完善及提供相關服務。惟個人生理資料或日常活動資料通常被認為是個人資料，導致一般民眾對上述應用感到不安，加上歐盟一般資料保護規範（General Data Protection Regulation, GDPR）施行後，加強對歐盟境內個資蒐集和利用之保護，亦影響到其他與歐盟有交易往來之國家，使得智慧建築資料相關法律問題變得越來越複雜，成為業者於建築物內導入相關應用之阻礙。

我國目前有關智慧建築之規範，以獎勵性質之智慧建築標章為主，內政部並訂有「智慧建築設計技術參考規範」，針對各類型建築物智慧化之共通部份，依設置標準加以分級規範，提供給智慧建築起造人、設計人、各專業技術及相關機關參考。除上述獎勵性標章及參考規範外，《建築技術規則》建築設計施工篇第四章之一「建築物安全維護設計」針對供公眾使用建築物之公共空間設置安全維護裝置設有規範，而上述安全維護裝置，如照明裝置、監視攝影裝置、緊急求救裝置和警戒探測裝置等，與智慧建築標章和「智慧建築設計技術參考規範」之安全防災指標相仿，故應可將《建築技術規則》有關建築物安全維護設計之規定，視為我國法上有關智慧建築之最低標準。

上述安全維護裝置中，由於監視攝影裝置會蒐集影像等個人資料，屢屢成為輿論關注重點。本問答集經訪談和舉辦座談會，徵集台北市政府都市發展局、保全業者和設備廠商、建商、建築師公會、智慧建築協會、物業管理學會、保全商業同業公會等產學研各界意見，發現利用門禁系統或監視攝影裝置資料，提供及完善建築物內部各項服務之需求與日俱增，如分析獨居長者平常進出大門時間和頻率，掌握住戶安全，避免獨居長者發生意外卻無人知悉等狀況發生。此外，對業者而言，由於業界普遍不熟悉個資法相關規範，可能會因為擔心蒐集及利用資料違反個資法，而影響其於建築物內導入相關設備之意願；對於一般民眾而言，可能會因為不清楚資料提供給誰、如何處理和利用資料、提供後資料將用於何處、對提供資料的人而言有什麼好處等問題，使其過於擔心個人資料被濫用而感到不安。

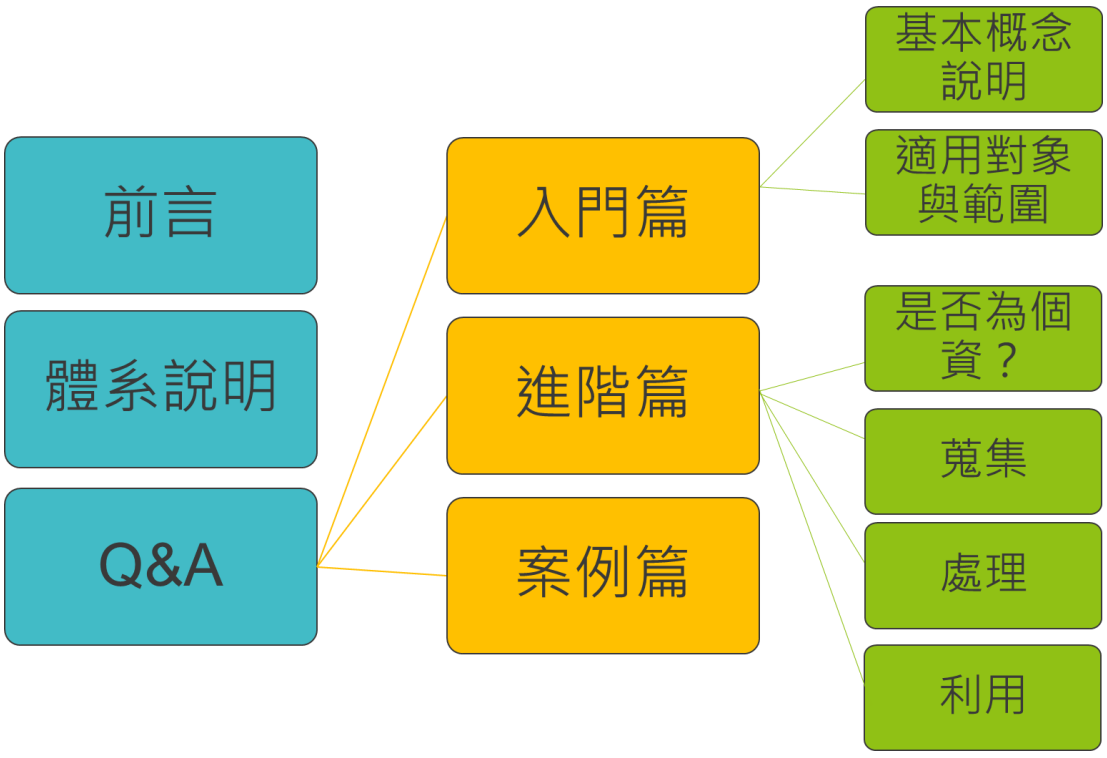
綜上所述，為鼓勵業者導入門禁系統或監視攝影裝置等設備，並降低一般民眾對

於業者分析、利用上述設備所蒐集資料之疑慮，以推動人工智慧等新技術應用於智慧化居住空間，內政部建築研究所委託資訊工業策進會科技法律研究所，參酌歐盟、日本等國家和地區有關促進監視攝影裝置資料利用之作法，編寫本問答集，提供各界參考。

二、使用說明

本問答集分為前言、使用說明和 Q&A 三個部份，Q&A 又可再分為入門篇、進階篇和案例篇。入門篇為基本概念說明和名詞解釋；進階篇根據資料應用流程，依序針對資料是否個人資料，以及個人資料之蒐集、處理和利用相關問題，以圖示或淺顯文字進行說明；案例篇則挑選數個門禁系統和監視攝影裝置在建築物內之應用情境，透過具體案例說明智慧建築資料應用之注意事項。如果對於資料將來的用途，以及門禁系統和監視攝影裝置裝設的地點和適用對象等問題，已經有基本構思的話，可以直接參考案例篇部份，看是否有接近的案例可以參考；如果對於未來可能會蒐集哪些資料，以及資料用途都還沒有具體概念的話，建議可以從入門篇開始，逐步了解智慧建築資料應用可能遭遇的問題。

本問答集整體架構如下：



三、入門篇

（一） 基本概念說明

Q1：什麼是智慧建築？

根據內政部「智慧建築標章申請認可評定及使用作業要點」第 2 點，智慧建築係指『**藉由導入資通訊系統及設備之手法，使空間具備主動感知之智慧化功能，以達到安全健康、便利舒適、節能永續目的之建築物。**』另內政部建築研究所《智慧建築評估手冊》在序言中指出『智慧建築是應用網路、監測設備及系統整合等技術，讓建築物達到自動感知、分析及回應等功能，並在規劃設計之初，事先考慮使用者需求,提供需要的服務及後續維護管理的方便性,使建築物在完成之後,可以有最佳化之組合與運轉，以滿足使用者對安全、舒適、便利、效率的需求，並達到節能與降低維護管理人力經費之目標。』綜上所述，可知**智慧建築是應用資通訊技術，使建築物可滿足使用者需求之建築物**。

Q2：什麼是供公眾使用之建築物？

根據《建築法》第 5 條，所謂供公眾使用之建築物，係指為供公眾工作、營業、居住、遊覽、娛樂及其他供公眾使用之建築物，參考台內營字第 0990801045 號令，其具體範圍如下：

十二、 戲院、電影院、演藝場。
十三、 舞廳（場）、歌廳、夜總會、俱樂部、加以區隔或包廂式觀光（視聽）理髮（理容）場所。
十四、 酒家、酒吧、酒店、酒館。
十五、 保齡球館、遊藝場、室內兒童樂園、室內溜冰場、室內游泳場、室內撞球場、體育館、說書場、育樂中心、視聽伴唱遊藝場所、錄影節目帶播映場所、健身中心、技擊館、總樓地板面積二百平方公尺以上之資訊休閒服務場所。
十六、 旅館類、總樓地板面積在五百平方公尺以上之寄宿舍。
十七、 總樓地板面積在五百平方公尺以上之市場、百貨商場、超級市場、休閒農場遊客休憩分區內之農產品與農村文物展示（售）及教育解說中心。
十八、 總樓地板面積在三百平方公尺以上之餐廳、咖啡廳、茶室、食堂。
十九、 公共浴室、三溫暖場所。
二十、 博物館、美術館、資料館、圖書館、陳列館、水族館、集會堂（場）。
二十一、 寺廟、教堂（會）、宗祠（祠堂）。
二十二、 電影（電視）攝影廠（棚）。
二十三、 醫院、療養院、兒童及少年安置教養機構、老人福利機構之長期照

護機構、安養機構（設於地面一層面積超過五百平方公尺或設於二層至五層之任一層面積超過三百平方公尺或設於六層以上之樓層者）、身心障礙福利機構、護理機構、住宿型精神復健機構。

二十四、　銀行、合作社、郵局、電信局營業所、電力公司營業所、自來水營業所、瓦斯公司營業所、證券交易場所。

二十五、　總樓地板面積在五百平方公尺以上之一般行政機關及公私團體辦公廳、農漁會營業所。

二十六、　總樓地板面積在三百平方公尺以上之倉庫、汽車庫、修車場。

二十七、　托兒所、幼稚園、小學、中學、大專院校、補習學校、供學童使用之補習班、課後托育中心、總樓地板面積在二百平方公尺以上之補習班及訓練班。

二十八、　都市計畫內使用電力（包括電熱）在三十七點五千瓦以上或其作業廠房之樓地板面積合計在二百平方公尺以上之工廠及休閒農場遊客休憩分區內總樓地板面積在二百平方公尺以上之自產農產品加工（釀造）廠、都市計畫外使用電力（包括電熱）在七十五千瓦以上或其作業廠房之樓地板面積合計在五百平方公尺以上之工廠及休閒農場遊客休憩分區內總樓地板面積在五百平方公尺以上之自產農產品加工（釀造）廠。

二十九、　車站、航空站、加油（氣）站。

三十、　殯儀館、納骨堂（塔）。

三十一、　六層以上之集合住宅（公寓）。

三十二、　總樓地板面積在三百平方公尺以上之屠宰場。

三十三、　其他經中央主管建築機關指定者。

Q3：建築物之公共空間是指哪些地方？

《建築技術規則》第四章之一規定公共空間需設置安全維護裝置，條文內所提到之空間包括：停車空間（室內/室外）、車道、車道出入口、機電設備空間出入口、電梯車廂內、安全梯間、屋突層機械室出入口、屋頂避難平台出入口、屋頂空中花園、公共廁所、室內公共通路走廊、基地內通路、排煙室、避難層門廳、避難層出入口。其中應設置監視攝影裝置之空間僅有停車空間（室內/室外）、車道、車道出入口和電梯車廂內，其餘空間視實際需求設置。

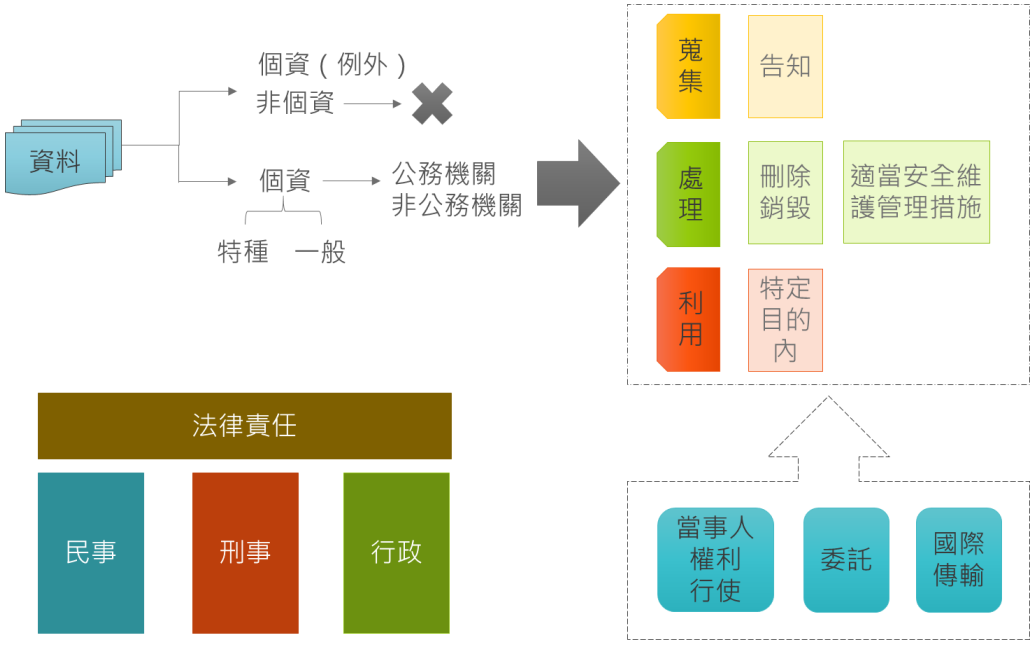
Q4：問答集所稱之門禁系統和安全監控設備是什麼？

本問答集所稱之門禁系統，係指建築物出入口或停車場出入口，利用刷卡、磁扣、指紋辨識、虹膜和人臉辨識等方式辨識身份之管制措施。社區內門禁系統常結合物業管理系統、中央監控系統或消防系統，以便發生火災或意外時能即時

啟動消防通道和安全門，或透過系統直接通知中央監控室報警。

建築物內安全監控設備分為設備監控和人物監控兩種，前者監視建築物內設備運轉狀況，後者則可進一步分為純影像拍攝、動態偵測和熱感應等類型。本問答集所稱之安全監控系統指人員監控，不包括設備監控在內。必須注意的是，部份安全監控設備係以監控場域本身為主，並非以拍攝人物為目的，只是在拍攝或紀錄場域狀況時，可能會拍攝到人物影像，針對上述狀況，由於會拍到人物，故仍算在人物監控類別。

Q5：我國個人資料保護法之規範架構。



Q6：什麼是個人資料？

根據《個人資料保護法》第 2 條第 1 項第 1 款，個人資料為自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。上述規定前段為例示規定，立法者以列舉方式，告訴民眾哪些資料為個人資料，而後段則直接表示「其他得以直接或間接方式識別該個人之資料」為個人資料，故只要符合後段定義者，縱使沒有列在前段，亦為我國《個人資料保護法》所稱之個人資料。由於只要「得以直接或間接方式識別該個人之資料」均為個人資料，故如何判斷系爭資料為個人資料，成為資料應用之重要前提。

Q7：什麼是一般資料和特種資料？

《個人資料保護法》第 6 條第 1 項規定：「有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。」上述列在條文中之個人資料即為特種資料，除符合例外情形，原則上不得蒐集、處理和利用，而非屬上述資料之個人資料即為一般資料，只要遵守《個人資料保護法》之規定，就可蒐集、處理和利用。

Q8：什麼是個人資料之蒐集、處理和利用？

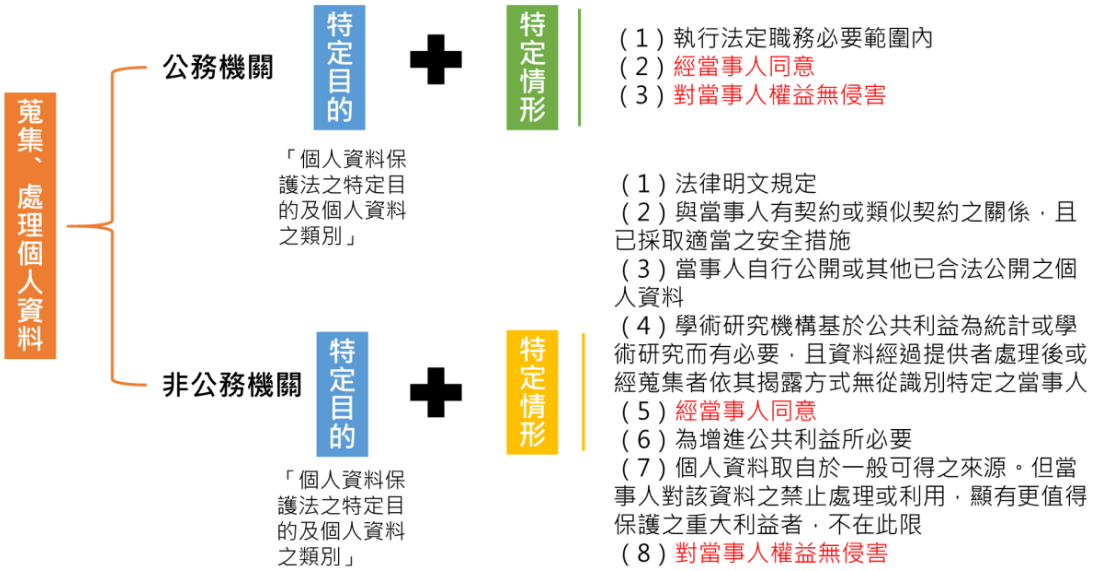
根據《個人資料保護法》第 2 條第 1 項第 3 款，蒐集指以任何方式取得個人資料。

所謂個人資料之處理，係指『為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送』等行為，而前述之個人資料檔案，則是指『依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。』

根據《個人資料保護法》第 2 條第 1 項 5 款，利用指將蒐集之個人資料為處理以外之使用。如分析個人資料或將個人資料用於電話行銷等。在利用個人資料時，如利用者為公務機關，利用之行為應於執行法定職務必要範圍內為之，並與蒐集時之特定目的相符；如利用者為非公務機關，則只要利用個人資料符合蒐集時之特定目的即可。

延伸閱讀：法務部法律字第 10503520020 號、法務部法律字第 10303511680 號

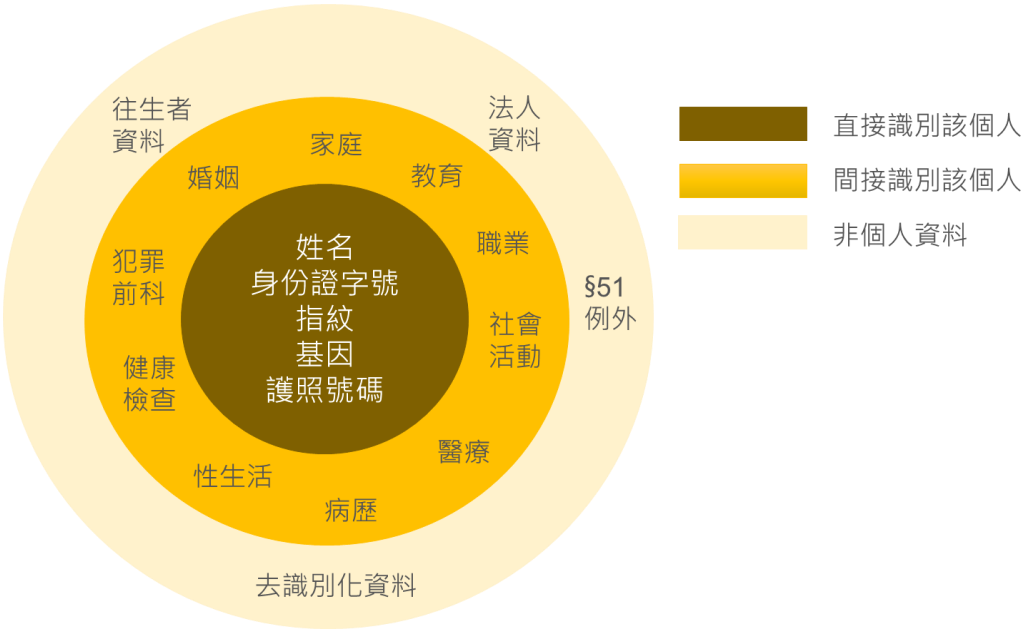
Q9：蒐集、處理個人資料應符合哪些特定目的和特定情形？



Q10：哪些個人資料不適用《個人資料保護法》？

《個人資料保護法》第 2 條第 1 項規定，個人資料指『**自然人**之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他**得以直接或間接方式識別該個人**之資料。』由此可知，只有得以識別該個人之自然人資料才是個人資料。換言之，非自然人，如往生者，或無法識別該個人之資料均不適用《個人資料保護法》。

此外，《個人資料保護法》第 51 條第 1 項規定：「有下列情形之一者，不適用本法規定：一、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。」故個人為舉辦同學會蒐集同學聯絡資料，或公司活動中所拍攝之尚未與其他資料結合之影片和照片，亦不適用《個人資料保護法》。



Q11：個人資料之去識別化是什麼意思？

所謂去識別化資料係指經處理後無法識別特定個人之資料。我國《個人資料保護法》並未明文定義去識別化以及去識別化方式，故有關去識別化標準，必須參考經濟部標準檢驗局於 2014 年 6 月和 2015 年 6 月公布之國家標準 CNS29100「資訊技術-安全技術-隱私權框架」，以及 CNS29191「資訊技術-安全技術-部分匿名及部份去連結鑑別之要求事項」。此外，經濟部標準檢驗局亦於 2019 年 2 月 20 日公布「資訊技術-安全技術-個人可識別資訊保護之作業規範」、「資訊技術-安全技術-個人可識別資訊去識別化過程管理系統-要求事項」草案，擬將個人資料去識別化處理之業者，可參考上述文件為之。

Q12：《個人資料保護法》規定蒐集、處理、利用個人資料需有特定目的或符合特定情形，特定目的和特定情形是指什麼？

蒐集個人資料除須告知當事人外，還應具有特定目的，換言之，不能毫無理由就隨便蒐集個人資料。關於蒐集個人資料之目的，必須在蒐集時一併告知當事人，同時需要說明所蒐集資料之類別。

關於蒐集資料之特定目的，以及個人資料之類別，可以參考「法務部個人資料保護法之特定目的及個人資料之類別」。至於公務機關和非公務機關蒐集資料所應符合之特定情形，則分別規定於《個人資料保護法》第 15 條及第 19 條。

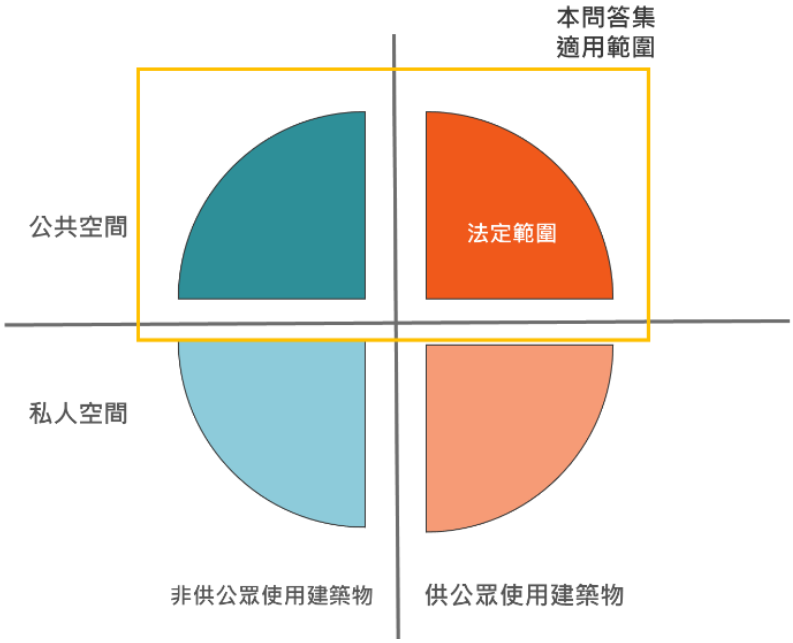
（一） 適用對象與範圍

Q13：本問答集之適用對象包括哪些人？

本問答集之適用對象包括可能會被門禁系統及監視攝影裝置蒐集資料之一般民眾，以及擬於建築物內導入監視攝影裝置之建築物所有人、建商、建築師、設備廠商、保全業者、不動產管理業等相關從業人員。未來業者可於導入相關系統或設備時，藉由本問答集向民眾說明以解消疑慮。

Q14：本問答集之適用範圍為何？

我國僅要求供公眾使用建築物之公共空間必須設置安全維護裝置，故本問答集適用範圍原則上以供公眾使用建築物之公共空間為主，惟考量到部份非供公眾使用建築物，如小型商店、餐飲店等，仍有在公共空間裝設監視攝影裝置之需求，故將其一併納入本問答集範圍，僅排除於建築物之私人空間，如個人於住家內外裝設監視攝影機，拍攝住家門口或周遭環境等情形。



此外，傳統建築物內設置監視攝影裝置，通常係以人員監控為目的，而門禁系統則是為管控人員進出，惟在智慧建築發展趨勢下，建築物內裝設上述設備之目的不再僅限於監視或場域管理，可能還有統計人數、性別、年齡、人流動線等其他目的。本問答集經訪談及參考國外文獻後，整理建築物內導入前述裝置之情境、資料類型和用途如下表：

表 3 門禁系統應用情境和資料用途

	應用情境	資料類型	資料用途
門禁系統	在建築物出入口設置門禁，個人必須透過刷卡、指紋、虹膜、人臉辨識等方式進行驗證，進入特定區域	使用人姓名（持卡人）、職稱、住家電話、行動電話、地址、身分證字號、統一編號、戶別、車牌和車位、出入時間和進出次數、聲音等個人資料	6. 場域進出管理 7. 掌握特定人進出履歷、時間、動線，用於提供個人化服務 8. 提供給其他單位（如檢調機關）

表 4 監視攝影裝置運用情境和資料用途

	應用情境	資料類型	資料用途
監視攝影裝置	拍攝公共區域內影像	公共區域內特定或不特定多數人，以及周遭環境影像資料	17. 場域安全監控 18. 紀錄場域狀況 19. 統計人數 20. 統計性別和年齡等人物特徵 21. 紀錄人物座標和人流動線 22. 統計分析上述資料之間的關聯性 23. 將影像資料與其他資料進行比對 24. 利用影像資料訓練 AI 或進行產品研發

綜上所述，**本問答集所適用之範圍，為裝設在公共空間之門禁系統和監視攝影裝置，且其裝設目的不僅限於場域進出管控或安全監控，包括蒐集、分析資料用於提供或優化各項服務在內**。在後續應用情境及案例分析中，本問答集將以上述資料用途為基礎，分別整理門禁系統和安全監控設備之應用情境。

一、進階篇

（一） 智慧建築資料之特徵及注意事項

Q15：門禁系統取得資料之特徵及注意事項。

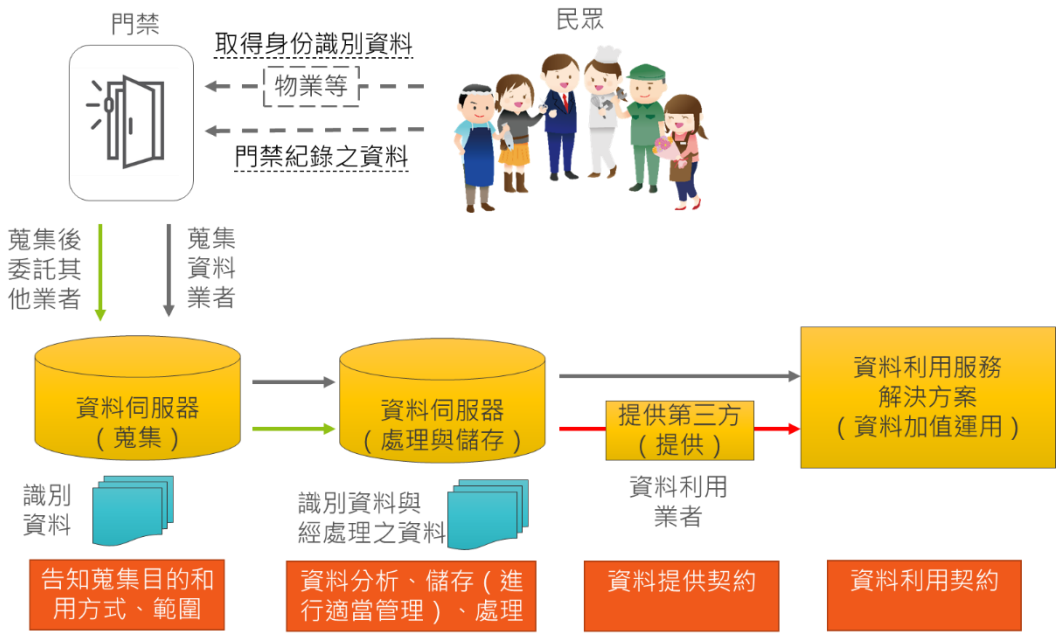
目前部份辦公大樓、集合式住宅，或其他需要管制進出之區域，會透過刷卡、指紋、虹膜、人臉辨識等方式進行身份驗證，而為進行驗證，必須取得當事人資料，方能在系統中進行比對，允許符合資格者進入管制區域，故**門禁系統通常會事先取得資料主體蒐集、處理、利用其個人資料之同意，以便將資料運用於場域進出管理。**

門禁系統蒐集資料之目的，在於管理特定場域之進出狀況，而根據我國《個人資料保護法》第 5 條：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」**故門禁系統所蒐集之資料，原則上不能用於場域進出管理以外之用途。**

除事先蒐集資料用於身份驗證外，伴隨大數據及智慧化服務發展，資料主體通過門禁系統時所產生之資料，如進出時間、次數等，亦可進一步用於優化物業管理服務品質，如社區管理單位分析獨居高齡者每日進出大門時間和次數，當其長時間未出現或沒有依照往常時間進出時，物業便可前往關切，了解住戶是否發生需要協助的狀況。**有鑑於此，為促進門禁系統所蒐集資料之應用，在事先取得資料主體蒐集、處理、利用資料同意時，還需讓其了解門禁系統會保留進出紀錄，而這些看似無用的資料，未來可能有其他用途。**

另外，建築物時常會有訪客出入，門禁系統可能也會需要蒐集訪客資料，除掌握訪客身份及管控其進出外，亦可透過知道訪客在幾點幾分通過門禁系統，從而推算出訪客會在什麼時候抵達目的地，以便安排人力在該地點等待。**由於訪客只能在進出場域當下才能告知並取得蒐集、處理、利用其個人資料之同意，故該如何落實《個人資料保護法》之告知義務，以及取得資料主體同意，且確保所取得之資料不會逾越比例原則之限制，成為需要注意的問題。**

Q16：門禁系統之資料應用流程。

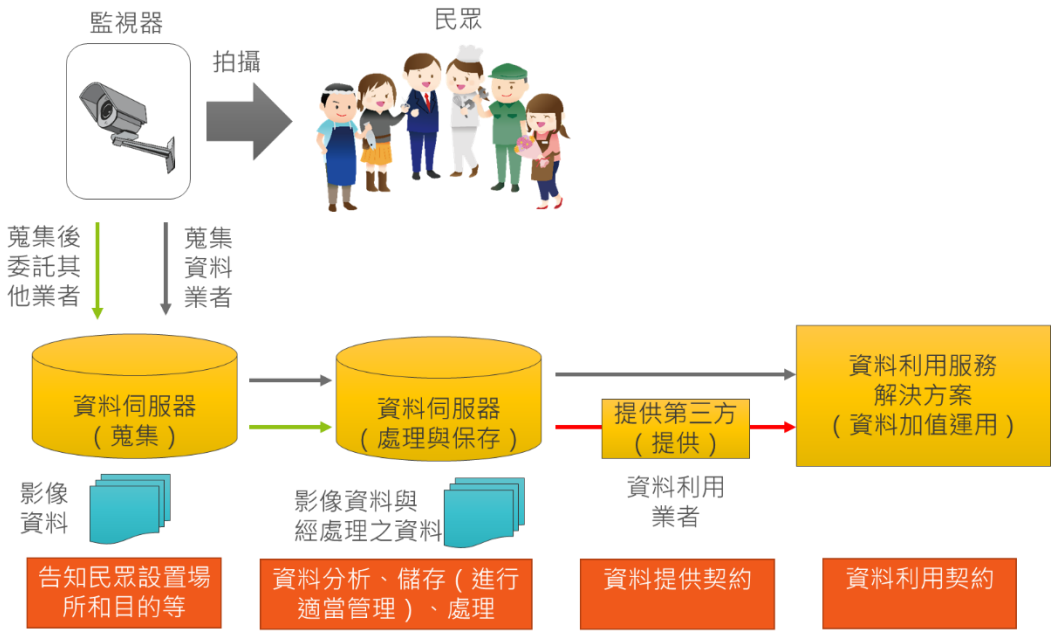


Q17：監視攝影裝置取得資料之特徵及注意事項。

根據《建築技術規則》第四章之一「建築物安全維護設計」，供公眾使用建築物之公共區域應設置安全維護裝置，而監視攝影裝置即為其中一種。除上述區域外，因應社區大樓內住戶或建築物使用者之需求，監視攝影裝置可能還會設置在其他區域，且用途並不僅限於安全監控，惟無論如何，由於監視攝影裝置本身具有設置地點隱密、不易被發現，事先很難取得資料主體同意等特性，故其取得資料時往往具備以下特徵：

- 根據拍攝範圍之設定及週邊環境影響，監視攝影裝置可能會拍到玻璃或鏡面中之反射影像，或經過建築物附近的路人，被拍攝之資料主體不一定知道自己會被拍攝，拍攝者也無法一一告知或取得被拍攝人同意。
- 對於被拍攝之資料主體而言，無法僅從監視攝影裝置外觀得知其設置之目的，以及所拍攝之影像資料將如何被運用。
- 監視攝影裝置可以紀錄資料主體的一舉一動，以及周遭環境變化，影像內存有龐大的資訊量，其中所透露之訊息可能已經逾越資料主體願意被蒐集的範圍，或資料主體根本沒有意識到可能會被蒐集。
- 伴隨技術進步，影像資料經進一步分析後，原先無意義的影像都有可能存在利用價值。

Q18：監視攝影裝置之資料應用流程。



Q19：門禁系統和監視攝影裝置之資料應用流程，一共可分為幾個階段？

門禁系統和監視攝影裝置資料在應用上，大致可分為蒐集、處理、利用三個階段，惟在進入上述階段前，尚須確認系爭資料是否為個人資料，以及資料類型等問題。在利用智慧建築資料前，應根據上述階段依序檢查各注意事項。

確認是否為個人資料

Q20：姓名、員工號碼、職稱、住家電話、行動電話、地址、身分證字號、統一編號、戶別、車牌和車位、聲音等.....門禁系統用來辨識身份之資料，是否為個人資料？

智慧建築內之門禁系統，為辨識特定人身份，可能會需要蒐集姓名、員工號碼、職稱、住家電話、行動電話、地址、身分證字號、統一編號、戶別、車牌和車位、聲音等資料，**上述資料因可直接或間接辨識出特定個人，故均該當我國法上之個人資料，在後續蒐集、處理及利用過程中，必須遵守我國《個人資料保護法》之規定。**

Q21：個人通過門禁系統之時間、次數等紀錄，是否為個人資料？

門禁系統會紀錄民眾進出時間和次數等資訊，**這些紀錄可以呈現特定個人日常生活的行動軌跡，與其他資料結合後亦有可能辨識出特定各人，故亦有該當個人資料之可能。**有鑑於此，門禁系統在取得及利用上述資料時，亦須注意《個人資料保護法》之規定。

惟單純紀錄進出次數之計數資料，如圖書館統計當日或當月入館人數，由於無法識別出特定個人，故非個人資料。

Q22：設置在公共區域之監視攝影裝置，如果只有拍攝建築物等風景，沒有拍攝到民眾，則是否仍為個人資料？

如果影像資料內沒有任何人，則非個人資料，無《個人資料保護法》之適用。

Q23：設置在公共區域之監視攝影裝置，如拍攝不特定之多數人影像（如設置在車站之監視器，每天都會拍到大量往來民眾），這些資料是否為個人資料？

雖然監視攝影裝置會拍攝到大量民眾影像，但這些影像所拍攝之對象為不特定多數人，**假使難以從影像中辨識出特定個人，則此種資料應非個人資料**，不適用《個人資料保護法》。必須注意的是，**假使能從影像中辨識出特定個人，如監視攝影裝置清楚地拍攝到人群中某人的臉部或身體特徵，與其他資料比對後可以知道對方是誰，則該影像資料仍有可能是個人資料。**

延伸閱讀：法務部法律字第 0999009760 號函釋

Q24：設置在公共區域之監視攝影裝置，如拍攝特定多數人之影像（如設置在集合式住宅內之監視器，原則上只會拍攝到社區住戶和訪客，故為「特定」多數人），這些資料是否為個人資料？

此種狀況與前者類似，然而雖然同樣會拍攝到許多人，**惟因可以特定出被拍攝人之身份，故在此種狀況下所拍攝之影像資料有該當個人資料之可能。**以問題中設置在集合式住宅內之監視攝影裝置為例，被拍攝人可能為住戶或訪客，前者每天都會出入集合式住宅，經比對住戶資料後就可確認身份，故為個人資料；而後者如果無法經由其他資料（如物業登記之訪客資料）比對後確認身份，則仍非個人資料。

Q25：設置在公共區域之監視攝影裝置，如拍攝特定人之影像，該資料是否為個人資料？

監視攝影裝置所拍攝之影像，**如拍攝到足以識別出特定個人之影像，**無論是拍到當事人正面或鏡面、玻璃窗中反射影像，均為個人資料，需要依照《個人資料保護法》規定蒐集、處理、利用。

Q26：如針對監視攝影裝置所拍攝之影像資料，擷取其中臉部影像或身體影像特徵，如臉上的疤痕、走路姿勢、體型等，上述經擷取之特徵影像是否為個人資料？

《個人資料保護法》第 2 條第 1 項規定，個人資料指『自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、**特徵**、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。』上述條文中明確指出「特徵」為個人資料，故這些資料雖然可能無法直接用以識別特定個人，但仍為個人資料。

Q27：根據特徵資料分析出之人物屬性，如具有某些特徵之人通常為男性或女性等，是否為個人資料？

在分析特徵資料歸納出某些性別、年齡或體型的人可能會具備之屬性後，**這些經分析、歸納出之人物屬性資料，如果沒有辦法回溯到特定個人身上，並非個人資料。**如擷取十位兒童全身影像，蒐集到每位兒童身高、胖瘦等體型特徵，這些特徵資料為個人資料；惟如進一步分析上述特徵資料，從而得知十位兒童平均身高和體重，由於平均身高和體重等數字無法和特定兒童連結在一起，故上述身高和

體重資料並非個人資料。

Q28：監視攝影裝置拍攝到之人物動線資料是否為個人資料？

人物動線資料為特定**個人之行動履歷**，可直接或間接識別出該個人，故為個人資料。

Q29：如果進一步將動線資料轉化為座標值，則該資料是否為個人資料？

如進一步分析動線資料，將其轉化座標值，如 2 點 50 分（255，370），則除非該座標值會與其他資料串連比對，否則無法僅從數字識別出該個人，故非個人資料。

Q30：門禁系統和監視攝影裝置所取得之資料是一般資料還是特種資料？

《個人資料保護法》第 6 條第 1 項規定：「有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。」上述列在條文中之個人資料即為特種資料，除符合例外情形，原則上不得蒐集、處理和利用，而非屬上述資料之個人資料即為一般資料，只要遵守《個人資料保護法》之規定，就可蒐集、處理和利用。

門禁系統所取得之資料，以及監視攝影裝置所拍攝之影像，只要不屬於上面所列之資料，即非特種資料。

（二） 蒐集資料時之注意事項

Q31：門禁系統和監視攝影裝置蒐集個人資料時可能遇到哪些問題？

無論係透過門禁系統或監視攝影裝置取得當事人資料，理論上都應遵守個資法規定，向當事人告知應告知事項。然而，要徹底落實上述規定並不容易，以門禁系統為例，如係事先針對住戶或員工等蒐集資料，自然可以清楚地告知當事人蒐集資料之目的、蒐集的資料類別、利用期間等.....事項，但如果是針對訪客當場進行告知，則恐怕難以清楚地向當事人說明或讓當事人理解告知的內容。如此一來，後續就有可能因雙方認知上的誤差而產生爭議。

再以監視攝影裝置為例，前面提到監視攝影裝置可能因為設置地點較隱密、拍攝範圍較廣，或可能拍攝到不特定多數人等原因，使得在拍攝時很難告知當事人。即便透過張貼告示等方式，向被拍攝人告知正在蒐集其影像資料，也無法確保所有人都會仔細閱讀告示或理解告示內容，故對欲導入相關設備之業者而言，該如

何落實《個人資料保護法》有關告知義務之規定，亦為急需解決的重要問題。

Q32：關於蒐集個人資料前要告知當事人之規定有無例外？如果門禁系統蒐集資料目的只是為驗證身份，或用於改善管理服務，是否不用告知當事人？

根據《個人資料保護法》第 8 條第 2 項規定，有 6 種例外情況可以免除告知義務：（1）依法律規定得免告知（2）公務機關為執行法定職務，或非公務機關為履行法定義務而蒐集資料（3）告知將妨害公務機關執行法定職務（4）告知將妨害公共利益（5）當事人明知應告知之內容（6）個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

如果門禁系統蒐集當事人資料只是為驗證其身份，或用以改善管理服務品質，並非出於營利考量，且對當事人無不利影響，理論上蒐集時不用告知當事人。

延伸閱讀：法務部法律字第 10503503290 號函釋、法務部法律字第 10403513100 號函釋、法務部法律字第 10203510680 號函釋、法務部法律字第 10100699790 號函釋

Q33：如果監視攝影裝置設置目的只是為監控場域安全，是否不用特別告知當事人？目前一般大樓或商場內都有設置監視器，理論上民眾應該都對此有所認識，是否符合不用告知的例外？

如果監視攝影裝置只是單純拍攝場域內影像，並非出於營利目的且對當事人無不利影響，則亦符合不用告知之例外。必須注意的是，雖然目前大樓或商場、停車場等地方通常都設有監視攝影裝置，民眾也知道會被拍攝，但僅從監視攝影裝置外觀及設置地點，無法知道是哪個單位在蒐集資料，也無從得知蒐集影像之目的、期間和用途等應告知內容，故恐怕無法以當事人明知告知內容為由，主張不用告知當事人。

Q34：如果蒐集之資料不是由當事人直接提供（業者只是間接取得），是否還需告知當事人？門禁系統和監視攝影裝置可能間接取得資料嗎？

假使資料不是由當事人提供，如蒐集當事人已經公開在網路上的電子郵件、公司電話等資料，在蒐集時不用告知當事人，直到要處理和利用資料時，才需要向當事人告知。必須注意的是，由於是間接取得當事人資料，故在進行上述告知時，必須向當事人說明資料來源。

此外，根據《個人資料保護法》第 9 條第 2 項，如果是（1）當事人自行公開或其他已合法公開之個人資料（2）不能向當事人或其法定代理人為告知（3）基於公共利益為統計或學術研究之目的而蒐集，且該資料經提供者處理後或蒐集者依其揭露方式，已無從識別特定當事人（4）大眾傳播業者基於新聞報導之公益目的而蒐集.....等情形，亦可免於向當事人為告知。

依照門禁系統和監視攝影裝置之運作方式，兩者都是直接蒐集當事人資料，理論上不太可能發生間接取得個人資料的問題。

延伸閱讀：法務部法律字第 10303511680 號函釋

Q35：在沒有辦法當面告知當事人，卻又不符合例外規定的狀況下，如商店在室內設置監視攝影裝置拍攝人流影像，作為日後改善結帳動線之資料時，店家該如何履行《個人資料保護法》有關告知之規定？

如果沒有辦法當面告知當事人，或許可以考慮在店門口或醒目處張貼告示，或透過廣播方式，讓當事人知道自己正在被蒐集資料。

Q36：門禁系統或監視攝影裝置蒐集資料可能符合哪些特定目的、另外，告知時還需要說明個人資料所屬之類別，個人資料有哪些類別？

門禁系統或監視攝影裝置蒐集資料，可能適用之特定目的包括：（〇〇七）不動產服務；（〇六九）契約、類似契約或其他法律關係事務；（〇七一）建築管理、都市更新、國民住宅事務；（一一六）場所進出安全管理；（一六四）營建業之行政管理；（一七六）其他自然人基於正當性目的所進行個人資料之蒐集處理及利用.....等。

此外，《個人資料保護法》亦規定個人資料之「蒐集和處理」必須符合特定情形，且根據蒐集單位是公務機關或非公務機關會有所不同。有關特定情形之問題，將一併在處理階段加以說明。

延伸閱讀：法務部法律字第 10403505690 號函釋

（三） 處理資料時之應注意事項

Q37：將監視攝影裝置或門禁系統所蒐集之個人資料編號後儲存在資料庫之行為，是「處理」個人資料嗎？

監視攝影裝置所拍攝之影像，門禁系統所蒐集之個人資料，如係為建立或利用個人資料檔案而儲存於資料庫內，都是處理個人資料之行為。

延伸閱讀：法務部法律字第 10103104550 號

Q38：想要蒐集、處理個人資料亦可透過取得當事人同意方式為之，關於表示同意之方式，《個人資料保護法》是否有所規定？

關於表示同意之方式，《個人資料保護法》針對蒐集、處理和利用有不同的規定。針對蒐集和處理，**當事人只要有表示出允許之意思即可**，就算不是非常明確的表示，只有點頭示意亦可。此外，雖然當事人什麼都沒講，但如果沒有明確表示反對並已提供個人資料，也可認為其同意我們蒐集、處理其個人資料。惟利用的狀況不同，**要利用個人資料必須取得當事人明確的表示**，不能只以當事人有點頭或沒表示反對為由，就認為對方已經同意我們利用其個人資料。

在取得當事人同意時，**原則上不以書面為限，只要當事人在被告知相關事項後表示同意即可。**然而病歷、醫療、基因、性生活、健康檢查及犯罪前科等特種資料之蒐集、處理和利用，就必須以書面取得當事人同意，且不能以當事人未表示反對為由，推定其已經同意，與一般資料不同。

（四） 利用資料時之應注意事項

Q39：監視攝影裝置蒐集個人資料原則上是為監控場域安全，如後來想進一步分析所蒐集之資料，如統計人數和分析動線，是否可能因不符合原先蒐集之目的，而違反《個人資料保護法》規定？

由於《個人資料保護法》要求利用個人資料須符合蒐集時之目的，故利用者不能隨便將蒐集來的個人資料拿去做其他用途。不過為促進個人資料之利用，《個人資料保護法》第 16 條和第 20 條，分別針對公務機關和非公務機關設有例外規定，清楚列出在符合哪些條件狀況下，可以為特定目的外之利用：

《個人資料保護法》第 16 條（針對公務機關）所規定之例外情況：（1）法律明

文規定（2）**為維護國家安全**或增進公共利益所必要（3）為免除當事人之生命、身體、自由或財產上之危險（4）為防止他人權益之重大危害（5）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經蒐集者依其揭露方式無從識別特定之當事人（6）有利於當事人權益（7）經當事人同意。

《個人資料保護法》第 20 條（針對非公務機關）所規定之例外情況：（1）法律明文規定（2）為增進公共利益所必要（3）為免除當事人之生命、身體、自由或財產上之危險（4）為防止他人權益之重大危害（5）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經蒐集者依其揭露方式無從識別特定之當事人（6）有利於當事人權益（7）經當事人同意。

綜觀上述規定，除公共機關可基於維護國家安全利用個人資料外，其餘規定大致相同，且就算都不符合例外狀況，只要取得當事人同意，仍然可以利用其個人資料。有鑑於此，即便一開始設置監視攝影裝置之目的與後來利用資料之目的不符，只要符合上述例外情形，仍然可以利用個人資料。

延伸閱讀：法務部法律字第 10503518090 號、法務部法律字第 10503512050 號

Q40：如果當事人表示同意，我們就可以在特定目的範圍外利用個人資料。此時的「同意」與當事人同意蒐集、處理個人資料，兩者有何不同？

根據《個人資料保護法》第 7 條第 2 項規定，在利用當事人個人資料時需要取得之同意，係指經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示。換言之，當事人必須明確表示同意，不能只以肢體動作（如點頭）就認為當事人已表示同意，或主張當事人沒有明確表示拒絕，故推測其已表示同意。

綜上所述，**如果門禁系統或監視攝影裝置只是單純蒐集、處理個人資料，則只要在告知當事人後，當事人有點頭或沒有明確拒絕並提供資料，就可以認為當事人同意我們蒐集、處理其個人資料；但如果要進一步利用所蒐集之個人資料，就需要得到當事人明確的回覆。此外，如果所蒐集到之資料為特種個資，就需要取得當事人書面同意。**

Q41：如建築物所有人或管委會係委託保全公司設置門禁和監視器，並保存相關資料於雲端或保全公司伺服器內，需要注意哪些事情？

《個人資料保護法》第 4 條規定：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」保全公司受建築物所有

人或管委會委託設置門禁系統和監視攝影裝置，蒐集個人資料，應根據上述規定，視委託者為公務機關或非公務機關，分別適用相關規定。

另外，《個人資料保護法施行細則》第 8 條規定，委託他人蒐集、處理或利用個人資料，**應對受託者為適當之監督，且須定期確認受託者執行狀況**。其監督事項至少應包含：（1）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（2）受託者就第十二條第二項採取之措施（3）有複委託者，其約定之受託者（4）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（5）委託機關如對受託者有保留指示者，其保留指示之事項（6）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。

Q42：檢調單位可否要求他人提供門禁資料或監視攝影裝置影像？

檢調單位為公務機關，蒐集或處理個人資料，應符合《個人資料保護法》第 15 條規定。根據上述條文規定，公務機關蒐集或處理個人資料應於「執行法定職務必要範圍內」，故若檢察機關係為偵辦案件而調取資料，屬於執行法定職務範圍，則應可依照《個人資料保護法》第 15 條第 1 款規定蒐集、處理個人資料。

Q43：向檢警提供門禁系統或監視攝影裝置所蒐集之資料，原則上為特定目的外利用，可以主張什麼理由讓提供行為合法？

向檢調單位提供門禁資料或監視攝影裝置影像之行為，理論上不在門禁系統或監視攝影裝置原先蒐集資料之目的範圍內，故必須符合《個人資料保護法》第 20 條規定所列之例外情形方可提供。《個人資料保護法》第 20 條第 1 項但書第 2 款規定：「為增進公共利益所必要」時，個人資料可以為特定目的外利用，檢察機關是為偵辦案件而調取資料，協助檢查機關辦案應符合「為增進公共利益所必要」，故可以依此為由，向檢查機關提供門禁資料或監視攝影裝置影像。

延伸閱讀：法務部法律字第 10703506760 號

Q44：住戶可否要求管委會刪除或停止蒐集、處理、利用門禁系統或監視攝影裝置內保存之個人資料？

根據個資法第 3 條，不可以預先與當事人約定拋棄或限制將來請求停止蒐集、處理、利用個人資料，或刪除個人資料之權利。在下列情況發生時，管委會應主動

或依當事人要求停止蒐集、處理、利用個人資料，或刪除個人資料：

1. 個人資料蒐集之特定目的消失或期限屆滿時。
2. 違反個資法規定蒐集、處理或利用個人資料。
3. 當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者。

四、案例篇

本問答集適用範圍包括供公眾使用之建築物和非供公眾使用之建築物公共區域，上述範圍內包括許多種類建築物，惟若從建築物類型出發整理應用情境，則可能因為裝設門禁系統和監視攝影裝置之目的重疊，導致整理出來的應用情境過於相似。有鑑於此，為清楚呈現智慧建築在資料應用過程中可能遭遇的問題，本問答集將從資料用途出發，於各種建築物中挑選具有代表性者作為範例進行說明。

（一） 門禁系統

1. 以紀錄出缺勤狀況為目的

辦公大樓

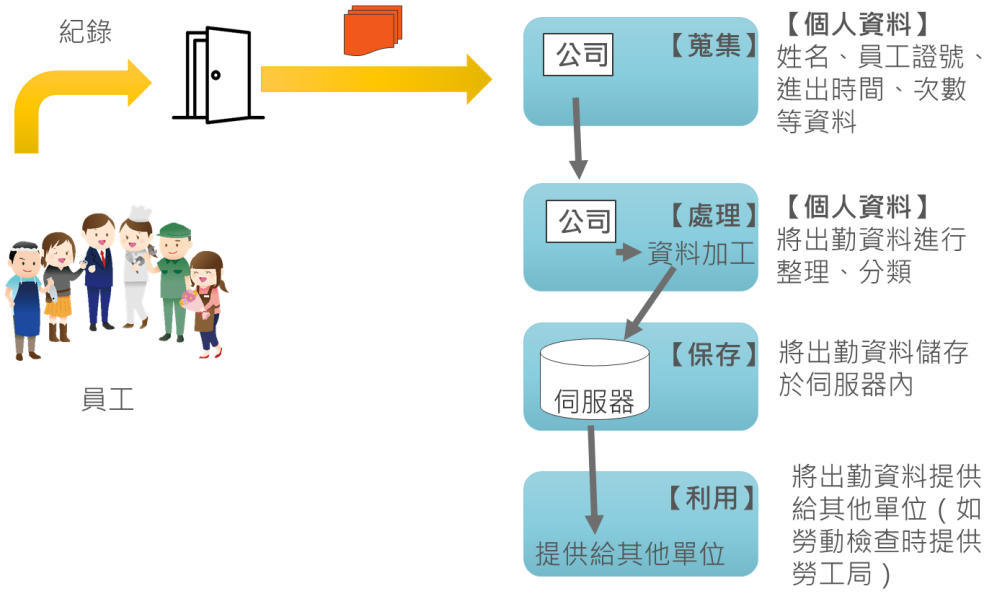
1 應用情境

	設置目的	設置區域	適用對象
門禁系統	出缺勤紀錄	辦公室門口	員工

2 蒐集資料

姓名、員工證號等身分識別資料。
進出門禁時間、次數等紀錄。

3 應用流程



辦公大樓內裝設門禁系統，除管控人員進出外，通常還會紀錄進出時間和次數等資料，紀錄出缺勤狀況，故適用對象為員工。門禁系統所蒐集之資料通常為可用以辨別當事人身分之姓名、員工證號、進出時間、次數等資料，而整個資料應用流程則如上圖所示。

為利用門禁系統驗證當事人身份，必須先蒐集當事人資料，然後將資料處理後儲存於伺服器內，等待當事人通過門禁系統時，再與當事人所持有之門禁卡、磁扣，或輸入之密碼、指紋等資料進行比對，驗證當事人身份。

在上述資料處理流程中，可能遭遇的問題包括：姓名、員工證號等資料是否為個人資料，以及蒐集、處理、利用個資時是否需要告知當事人及取得當事人同意等。門禁系統所蒐集之資料，由於可直接或間接用於識別該個人，故為個人資料，蒐集時應告知當事人蒐集單位、利用目的、方式、範圍等應告知事項，且在蒐集、處理時需要符合特定目的和特定情形。公司設置門禁系統蒐集當事人資料時，通常會與當事人間有契約或類似契約關係，且這些資料只是用於驗證身份或紀錄出缺勤狀況，並非出於營利考量而蒐集，且對當事人無不利影響，故不用再特別告知當事人。最後，在個人資料之利用上，由於門禁系統蒐集資料之目的是為管理場域進出，故只要將資料用於上述目的即可。

如果無法符合上述有關特定目的和特定情形之要求，則應取得當事人處理和利用個人資料之同意。具體說明可進一步參照下圖：

2. 以提供個人化服務為目的

集合式住宅

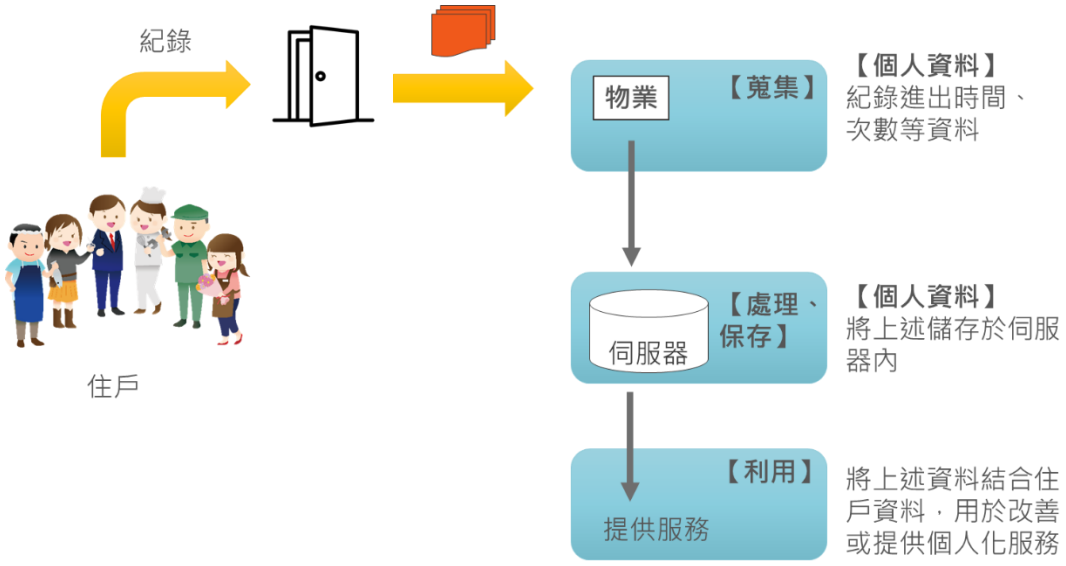
1 應用情境

	設置目的	設置區域	適用對象
門禁系統	提供個人化服務	建築物進出口	住戶、訪客

2 蒐集資料

姓名、戶別、地址、電話、身份證字號等身分識別資料。
進出門禁時間、次數等紀錄。

3 應用流程



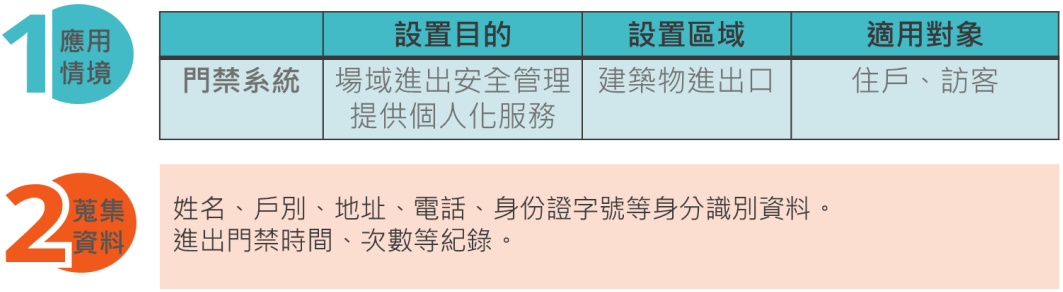
集合式住宅之住戶或訪客於通過門禁系統時，系統會留下通過時間和次數等紀錄，這些紀錄雖然不是可以直接用於識別個人之資料，但這些資料可以呈現出一個人日常生活的軌跡，再與其它資料結合後，若足以用於識別出特定個人，仍然有可能被認為是個人資料。

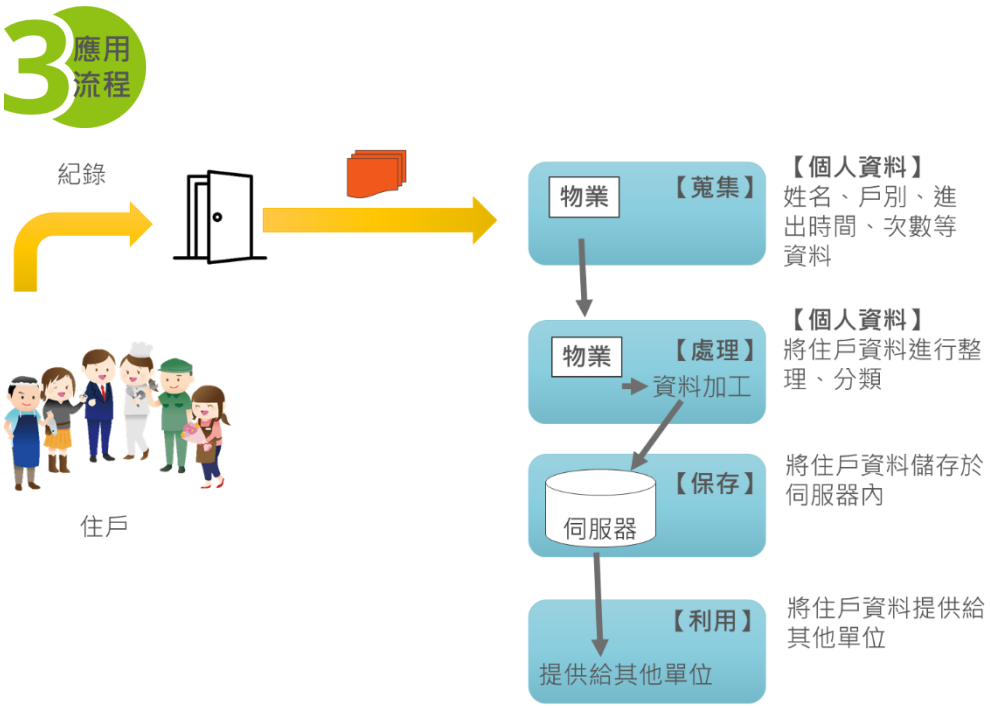
由於上述資料可能是個人資料，故蒐集、處理、利用仍須注意是否符合《個人資料保護法》規定。在蒐集個人資料時，原則上需要告知當事人蒐集單位、利用目的、方式、範圍等應告知事項，惟若蒐集資料並非出於營利考量或對當事人有不利影響等因素，則不用特別告知當事人。另外，在蒐集和處理個人資料時應符合特定目的和特定情形，門禁系統紀錄上述資料，如果是為改善或提供物業管理服務，可能符合「場域進出安全管理」、「不動產服務」或「消費者、客戶管理與服

務」等特定目的；若當事人與物業間有契約或類似契約關係，則亦符合特定情形之要求

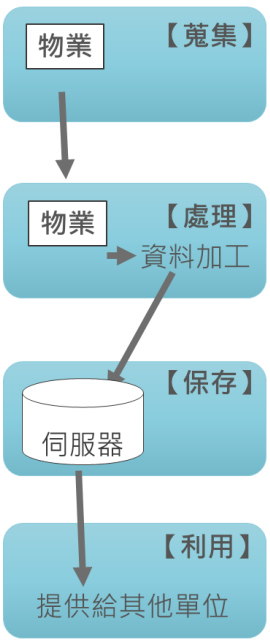
最後，在個人資料之利用上，必須要注意利用時須符合蒐集時之目的，如果逾越原先蒐集時之目的，則應取得當事人同意。具體說明可進一步參照下圖：

3. 以提供給其他單位為目的





一般而言，集合式住宅內門禁系統蒐集的資料，可能用於場域進出安全管理或提供物業管理服務，但通常不是為了將資料提供給別人而蒐集，故若有其他人或單位向持有上述資料的人要求提供資料時，就有可能涉及特定目的外利用，必須檢視是否符合個資法第 16 條或第 20 條之例外情形，或取得當事人利用其個資之同意，否則不能將資料提供給他人。具體說明可參照下圖：



	個資法規定	應注意事項
【個人資料】蒐集住戶資料	應告知當事人應告知事項	蒐集非出於營利目的，且對當事人無不利影響，故毋需告知
【個人資料】將住戶資料進行整理、分類	符合特定目的+特定情形	目的：場域進出管理 情形：與當事人有契約或類似契約之關係，且已採取適當之安全措施/取得當事人同意
將住戶資料儲存於伺服器內	符合特定目的+特定情形	同上
將住戶資料提供給其他單位	特定目的範圍內為之	檢查是否符合個資法第16條或第20條所列之例外情形

（二） 監視攝影裝置

1. 以監控場域安全為目的

車站、捷運站

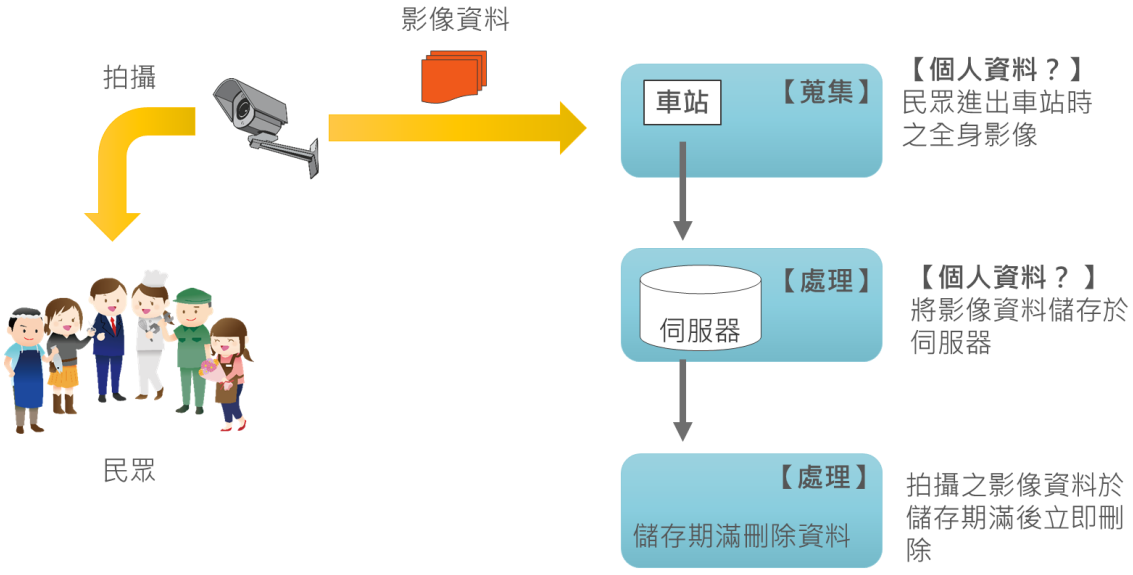
1 應用情境

	設置目的	設置區域	適用對象
監視攝影裝置	監控場域安全	停車空間 車道 車道出入口 電梯車廂內 安全梯間 屋頂空中花園 公共廁所 室內公共通路走廊 基地內通路 排煙室 避難層門聽 避難層出入口	進出車站之民眾

2 蒐集資料

不特定多數人影像資料。

3 應用流程

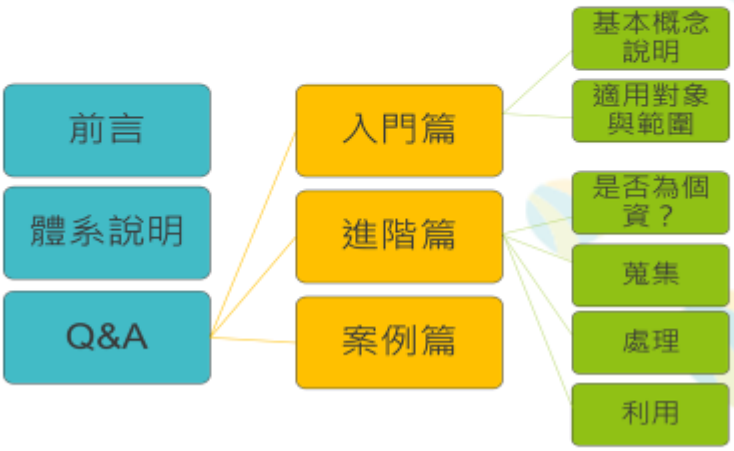


根據《建築技術規則》第四章之一，供公眾使用建築物之公共空間應設置安全維護裝置，故車站或捷運站等場所必須於停車空間、車道、車道出入口、電梯車廂內等處設置監視攝影裝置（部份場所非必須設置）。設置在上述場所之監視攝影裝置，可以拍攝到場域及往來民眾之全身影像，惟因拍攝到的影像為不特定多數人，在能辨識出特定個人前，理論上並非個人資料。

假使上述影像不是個人資料，則不適用《個人資料保護法》規定，業者在蒐集、處理、利用上述資料時不會受到法規限制。然而若上述影像資料有清楚地拍攝到人物長相，或可與其他資料結合後辨識出特定個人，則仍有可能被認為是個人資料，此時就需要遵守《個人資料保護法》，惟拍攝影像資料通常對當事人權益無侵害，且監控場域安全亦有可能解釋為增進公共利益所需，故其蒐集與處理應符合《個人資料保護法》規定。具體說明可參照下圖：

附錄十六：問答集草案第三版

本問答集分為前言、使用說明和Q&A三個部份，Q&A又可再分為入門篇、進階篇和案例篇。入門篇為基本概念說明和名詞解釋；進階篇根據資料應用流程，依序針對資料是否個人資料，以及個人資料之蒐集、處理和利用相關問題，以圖示或淺顯文字進行說明；案例篇則挑選數個門禁系統和監視攝影裝置在建築物內之應用情境，透過具體案例說明智慧建築資料應用之注意事項。



1 2020 資訊工業策進會 Institute for Information Industry

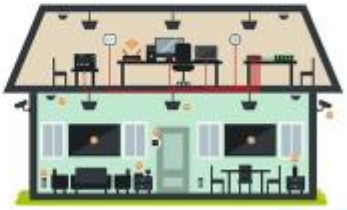
入門篇

基本概念說明

2 2020 資訊工業策進會 Institute for Information Industry

問1：什麼是智慧建築？

智慧建築是藉由導入資通訊系統及設備，達到安全健康、便利舒適、節能永續等目的，以滿足使用者需求之建築物。



*圖片僅為示意圖

參考條文：內政部「智慧建築標章申請認可評定及使用作業要點」第2點
延伸閱讀：內政部建築研究所《智慧建築評估手冊》

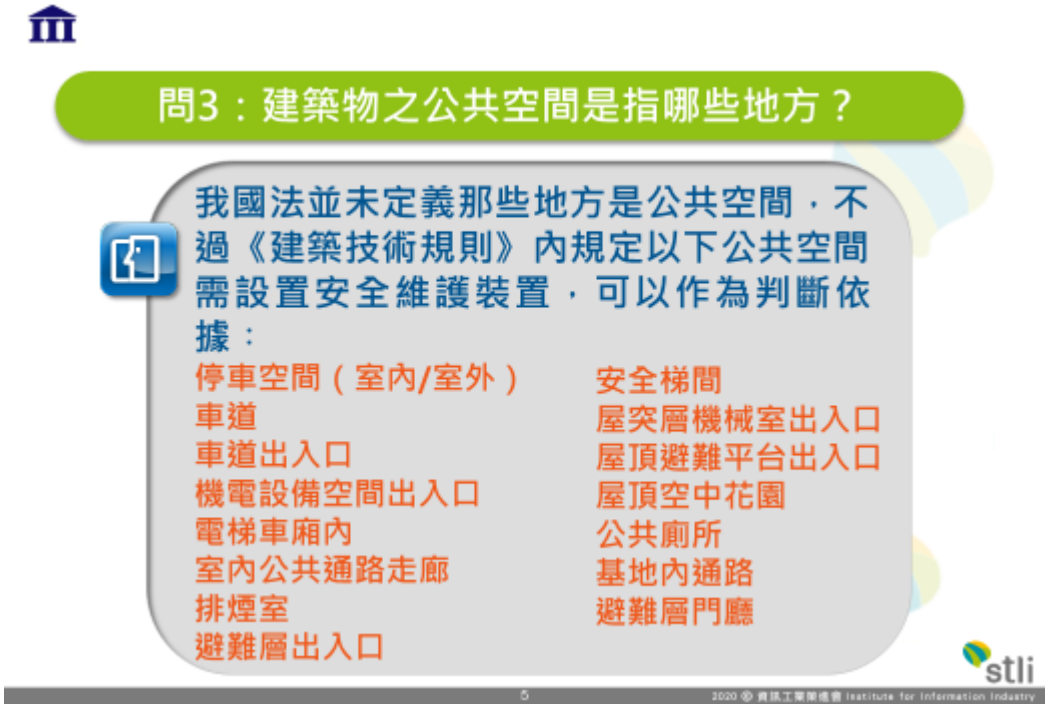
stli

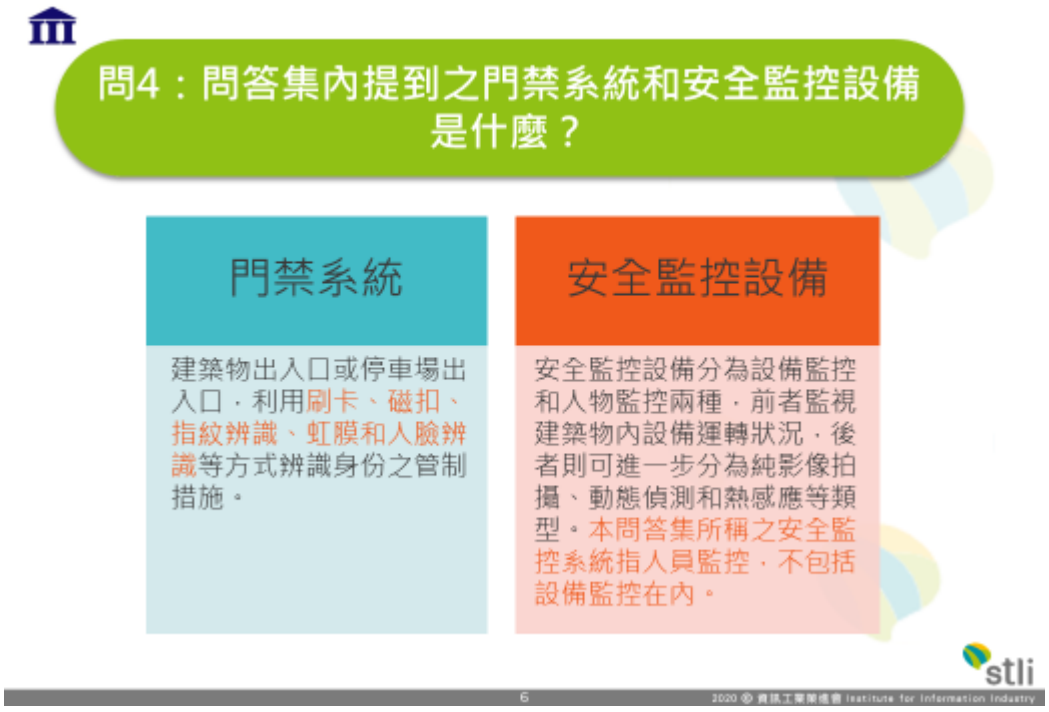
問2：什麼是供公眾使用之建築物？

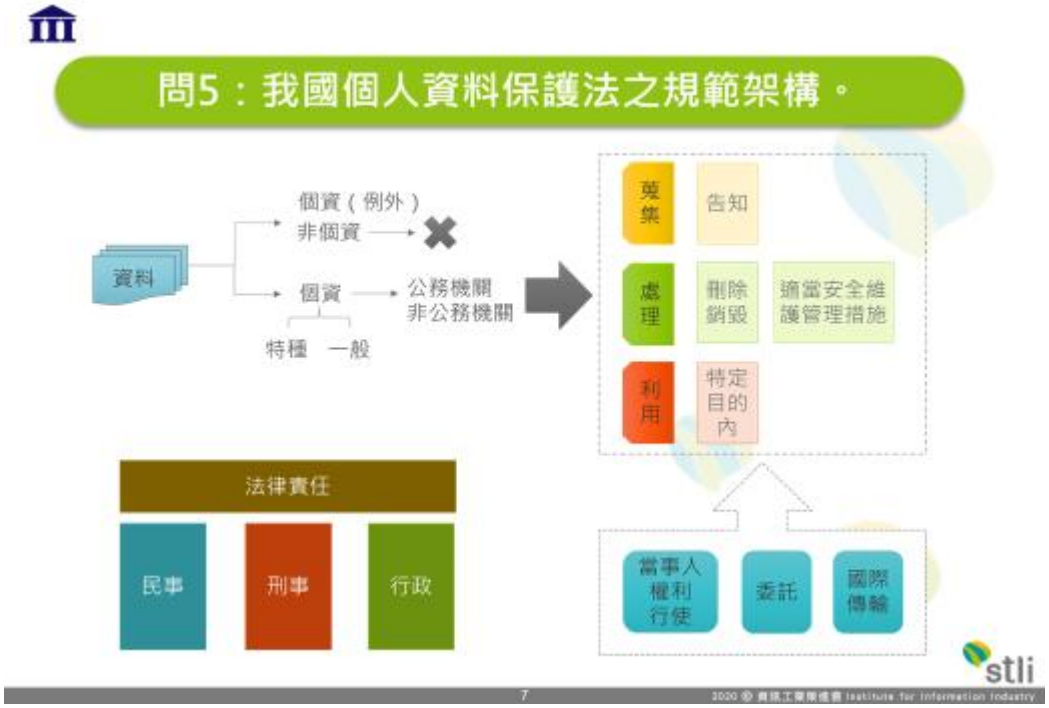
所謂供公眾使用之建築物，指為供公眾工作、營業、居住、遊覽、娛樂及其他供公眾使用之建築物。

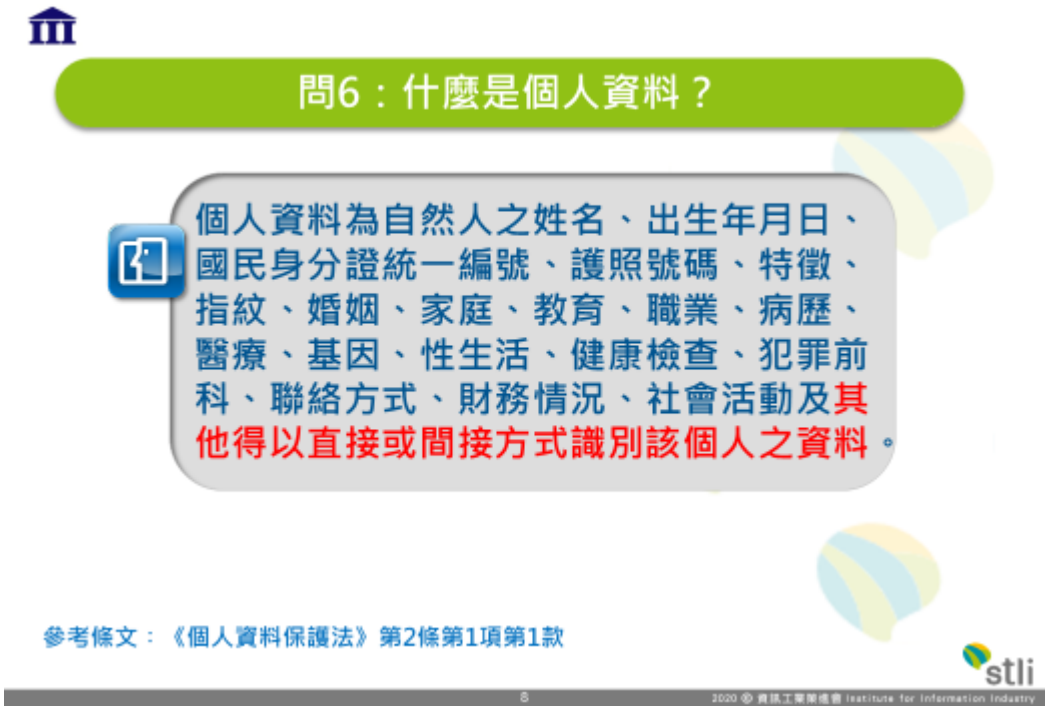
參考條文：《建築法》第5條
延伸閱讀：台內營字第0990801045號令

stli


問3：建築物之公共空間是指哪些地方？
我國法並未定義那些地方是公共空間，不過《建築技術規則》內規定以下公共空間需設置安全維護裝置，可以作為判斷依據：
停車空間（室內/室外）
車道
車道出入口
機電設備空間出入口
電梯車廂內
室內公共通路走廊
排煙室
避難層出入口
安全梯間
屋突層機械室出入口
屋頂避難平台出入口
屋頂空中花園
公共廁所
基地內通路
避難層門廳
stli
5
2020 資訊工業策進會 Institute for Information Industry


問4：問答集內提到之門禁系統和安全監控設備是什麼？
門禁系統
建築物出入口或停車場出入口，利用刷卡、磁扣、指紋辨識、虹膜和人臉辨識等方式辨識身份之管制措施。
安全監控設備
安全監控設備分為設備監控和人物監控兩種，前者監視建築物內設備運轉狀況，後者則可進一步分為純影像拍攝、動態偵測和熱感應等類型。本問答集所稱之安全監控系統指人員監控，不包括設備監控在內。
stli
6
2020 資訊工業策進會 Institute for Information Industry


問5：我國個人資料保護法之規範架構。
個資（例外）
非個資
資料
個資
公務機關
非公務機關
特種
一般
蒐集
告知
處理
刪除
銷毀
適當安全維護管理措施
利用
特定目的內
法律責任
民事
刑事
行政
當事人權利行使
委託
國際傳輸
stli
7


問6：什麼是個人資料？
個人資料為自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。
參考條文：《個人資料保護法》第2條第1項第1款
stli
8

問7：什麼是一般資料和特種資料？

上述6種資料「特種個資」，原則上不得蒐集、處理和利用。除此以外的個資為一般資料。

參考條文：《個資法》第6條第1項

問8：什麼是個人資料之蒐集、處理和利用？

蒐集

以任何方式取得個人資料。

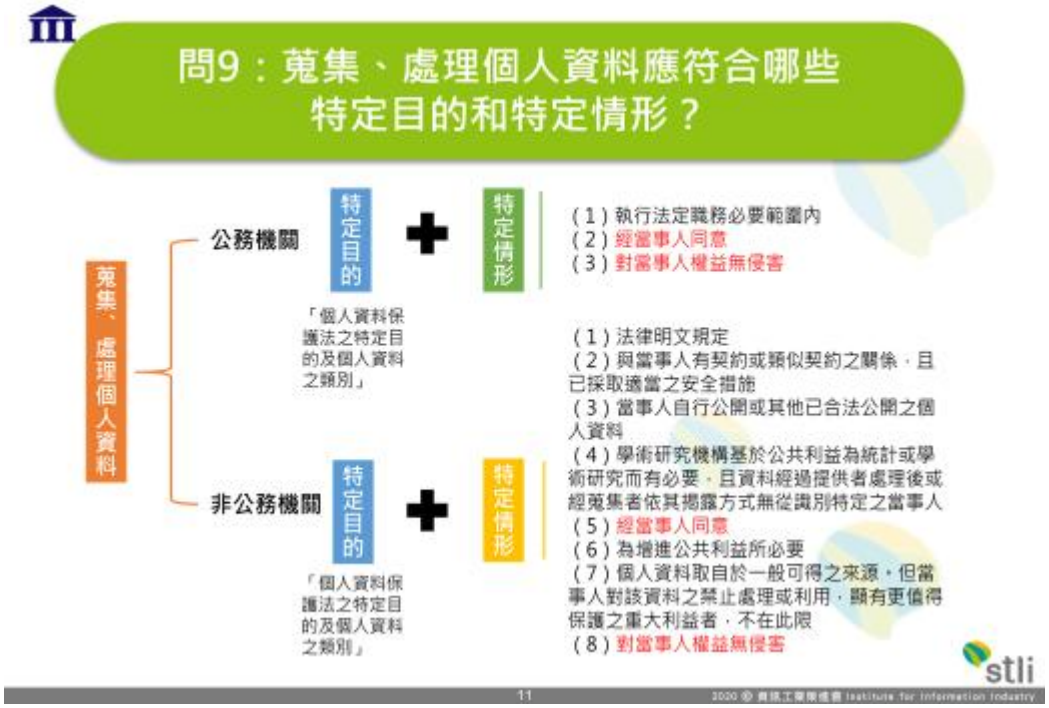
處理

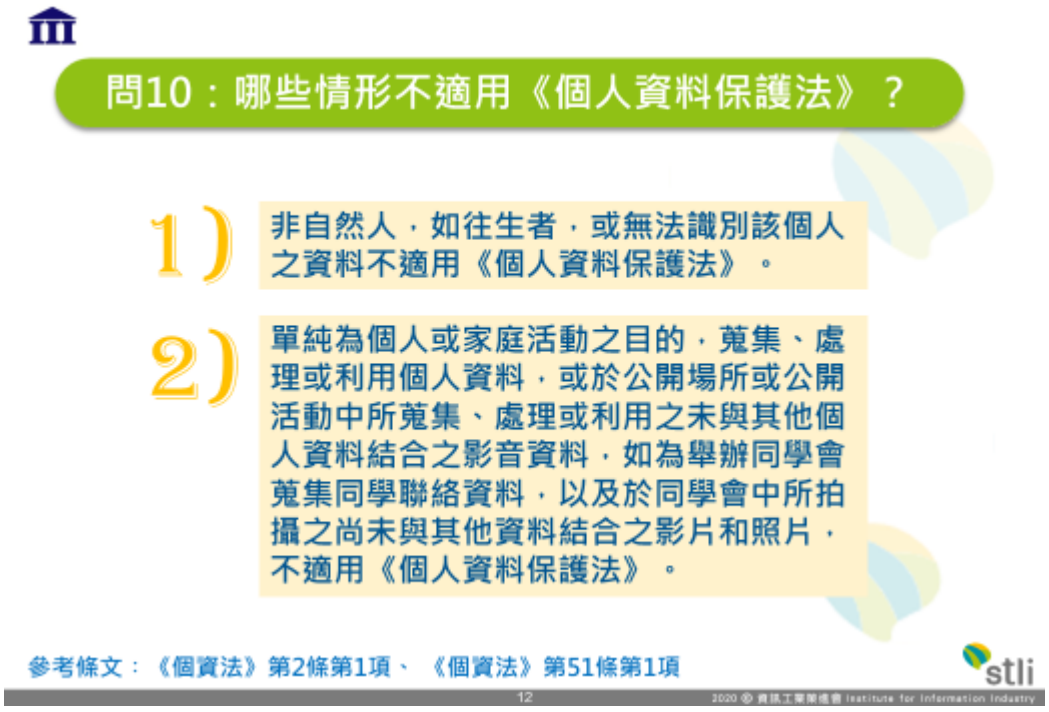
為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送』等行為。

利用

處理以外之使用。

參考條文：《個資法》第2條第1項第3~5款
延伸閱讀：法務部法律字第10503520020號、法務部法律字第10303511680號


問9：蒐集、處理個人資料應符合哪些特定目的和特定情形？
蒐集、處理個人資料
公務機關
特定目的
「個人資料保護法之特定目的及個人資料之類別」
特定情形
（1）執行法定職務必要範圍內
（2）經當事人同意
（3）對當事人權益無侵害
非公務機關
特定目的
「個人資料保護法之特定目的及個人資料之類別」
特定情形
（1）法律明文規定
（2）與當事人有契約或類似契約之關係，且已採取適當之安全措施
（3）當事人自行公開或其他已合法公開之個人資料
（4）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經蒐集者依其揭露方式無從識別特定之當事人
（5）經當事人同意
（6）為增進公共利益所必要
（7）個人資料取自於一般可得之來源，但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限
（8）對當事人權益無侵害
stli
11


問10：哪些情形不適用《個人資料保護法》？
1）
非自然人，如往生者，或無法識別該個人之資料不適用《個人資料保護法》。
2）
單純為個人或家庭活動之目的，蒐集、處理或利用個人資料，或於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料，如為舉辦同學會蒐集同學聯絡資料，以及於同學會中所拍攝之尚未與其他資料結合之影片和照片，不適用《個人資料保護法》。
參考條文：《個資法》第2條第1項、《個資法》第51條第1項
stli
12

問11：個人資料之去識別化是什麼意思？

去識別化資料係指**經處理後無法識別特定個人之資料**。

參考標準：國家標準CNS29100「資訊技術-安全技術-隱私權框架」、CNS29191「資訊技術-安全技術-部分匿名及部份去連結鑑別之要求事項」「資訊技術-安全技術-個人可識別資訊保護之作業規範」、「資訊技術-安全技術-個人可識別資訊去識別化過程管理系統-要求事項」草案

入門篇

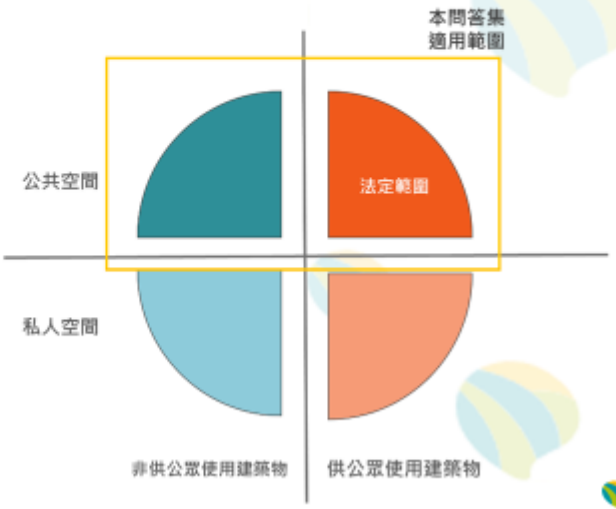
適用對象與範圍

問12：本問答集之適用對象。

適用對象包括可能會被門禁系統及監視器蒐集資料之**一般民眾**，以及擬於建築物內導入監視器之**建築物所有人、建商、建築師、設備廠商、保全業者、不動產管理業等相關從業人員**。未來業者可於導入相關系統或設備時，藉由本問答集向民眾說明以解消疑慮。

問12：本問答集之適用範圍。

我國僅要求供公眾使用建築物之公共空間必須設置安全維護裝置，故本問答集適用範圍原則上以供公眾使用建築物之公共空間為主。惟部份非供公眾使用建築物，如小型商店、餐飲店等，仍有在公共空間裝設監視器之需求，故將其一併納入本問答集範圍，僅排除於建築物之私人空間，如個人於住家內外裝設監視攝影機，拍攝住家門口或周遭環境等情形。



問13：門禁系統應用情境和資料用途。

	應用情境	資料類型	資料用途
門禁系統	在建築物出入口設置門禁，個人必須透過刷卡、指紋、虹膜、人臉辨識等方式進行驗證，進入特定區域。	使用人姓名（持卡人）、職稱、住家電話、行動電話、地址、身分證字號、統一編號、戶別、車牌和車位、出入時間和進出次數、聲音等個人資料。	1. 場域進出管理。 2. 掌握特定人進出履歷、時間、動線，用於提供個人化服務。 3. 提供給其他單位（如檢調機關）。

stli

17 2020 資訊工業策進會 Institute for Information Industry

問14：門禁系統應用情境和資料用途。

	應用情境	資料類型	資料用途
監視攝影裝置	拍攝公共區域內影像。	公共區域內特定或不特定多數人，以及周遭環境影像資料。	1. 場域安全監控。 2. 紀錄場域狀況。 3. 統計人數。 4. 統計性別和年齡等特徵 5. 紀錄人物座標和人流動線。 6. 統計分析上述資料之間的關聯性。 7. 將影像資料與其他資料進行比對。 8. 利用影像資料訓練AI或進行產品研發。

stli

18 2020 資訊工業策進會 Institute for Information Industry

進階篇

智慧建築資料之特徵及注意事項

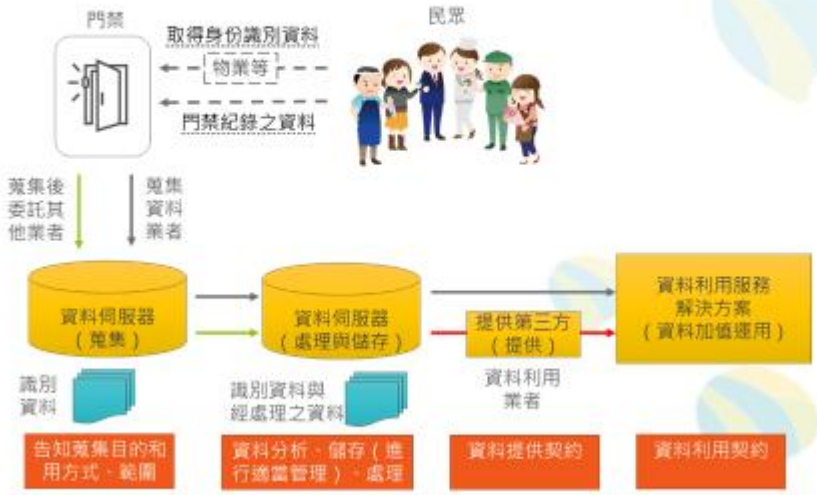
問15：門禁系統取得資料之特徵及注意事項。

1) 門禁系統通常會事先取得資料主體蒐集、處理、利用其個人資料之同意，以便將資料運用於場域進出管理。

2) 除事先蒐集資料用於身份驗證外，伴隨大數據及智慧化服務發展，當事人通過門禁系統時所產生之資料，如進出時間、次數等紀錄，亦可結合其他系統，用於提供額外服務。

3) 建築物還會有訪客出入，由於訪客只能在進出當下告知並取得蒐集、處理、利用其個人資料之同意，故該如何落實《個人資料保護法》規範，成為需要注意的問題。

問16：門禁系統之資料應用流程。



stli

問17：監視器取得資料之特徵及注意事項。

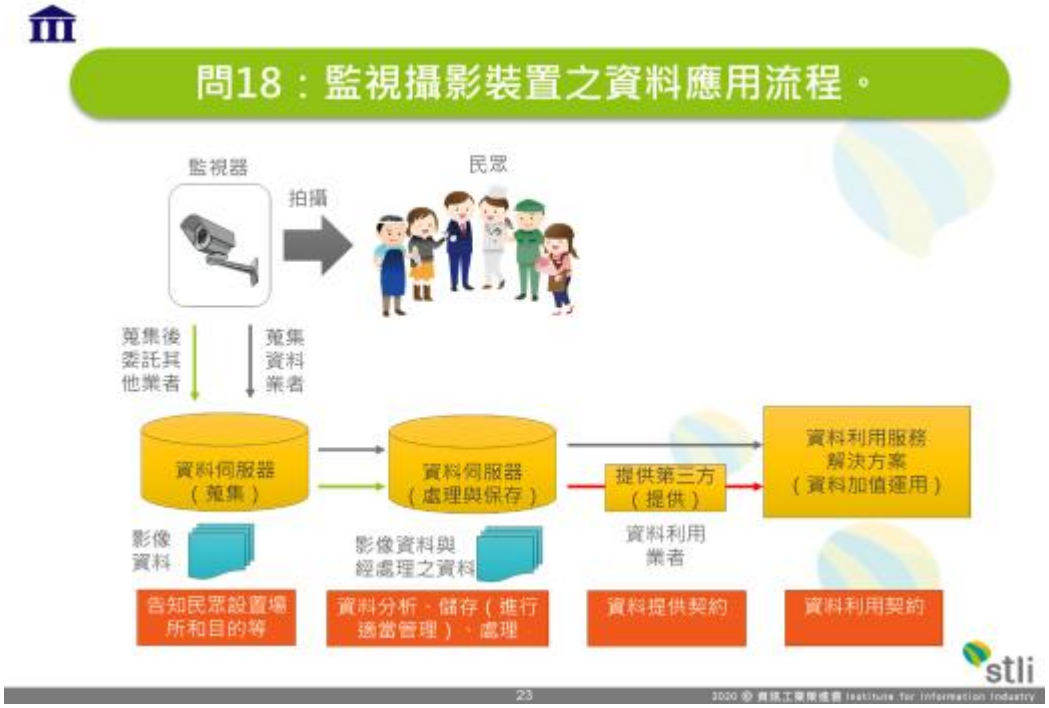
1) 被拍攝之當事人不一定知道自己會被拍攝，拍攝者也無法一一告知或取得被拍攝人同意。

2) 對被拍攝之當事人而言，無法僅從監視器外觀得知其設置之目的，以及所拍攝之影像資料將如何被運用。

3) 監視器可以紀錄當事人的一舉一動，以及周遭環境變化，影像內存有龐大的資訊量，其中所透露之訊息可能已經逾越當事人願意被蒐集的範圍。

4) 伴隨技術進步，影像資料經進一步分析後，原先無意義的影像都有可能存在利用價值。

stli


問18：監視攝影裝置之資料應用流程。
監視器
拍攝
民眾
蒐集後委託其他業者
蒐集資料業者
資料伺服器（蒐集）
資料伺服器（處理與保存）
提供第三方（提供）
資料利用服務解決方案（資料加值運用）
影像資料
影像資料與經處理之資料
資料利用業者
告知民眾設置場所和目的等
資料分析、儲存（進行適當管理）、處理
資料提供契約
資料利用契約
stli
23
2020 資訊工業策進會 Institute for Information Industry


問19：門禁系統和監視器之資料應用流程，可分為幾個階段？
確認是否為個資
蒐集
處理
利用
本問答集接下來將依照上述流程，依序整理各階段可能涉及之問題。
stli
24
2020 資訊工業策進會 Institute for Information Industry

問20：門禁系統用來辨識身份之資料，是否為個資？

門禁系統為辨識特定人身份，可能會需要蒐集姓名、員工號碼、職稱、住家電話、行動電話、地址、身分證字號、統一編號、戶別、車牌和車位、聲音等資料，上述資料因可直接或間接辨識出特定個人，故均為個人資料，在後續蒐集、處理及利用過程中，必須遵守《個人資料保護法》。

參考條文：《個人資料保護法》第2條第1項第1款

問21：個人通過門禁系統之時間、次數等紀錄，是否為個資？

門禁系統會紀錄民眾進出時間和次數等資訊，這些紀錄可以呈現特定個人日常生活的行動軌跡，與其他資料結合後亦有可能辨識出特定各人，故亦有該當個人資料之可能。惟單純紀錄進出次數之計數資料，如圖書館統計當日或當月入館人數，由於無法識別出特定個人，故非個人資料。

重點在於能不能單從資料本身，或將所取得之資料與其他資料串連比對後，知道當事人是誰！

問22：如果監視器只有拍攝到風景，還是個資嗎？

如果拍到的影像內沒有任何人，就只是單純的影像資料，不是個人資料。

*圖片僅為示意圖

單純的建築物或風景照片，不涉及個人資料

stli

27 2020 資訊工業策進會 Institute for Information Industry

問23：如果監視器拍攝到不特定多數人影像，這些影像是否為個資？

設置在車站之監視器，每天都會拍到許多進出民眾，由於人數眾多，且事先也很難知道誰會被拍到，**假使無法從影像中辨識出特定個人，則該影像應非個資。如果能從影像中辨識出特定個人，**如清楚拍到某人的臉部或身體特徵，與其他資料比對後可以知道對方是誰，**則影像資料仍有可能是個資。**

*圖片僅為示意圖

stli

28 2020 資訊工業策進會 Institute for Information Industry

問24：如果監視器拍攝到特定多數人影像，這些影像是否為個資？

設置在集合式住宅之監視器，每天都會拍到住戶進出，由於知道住戶是哪些人，可以特定出被拍攝人之身份，故影像資料有可能是個資。如果被拍到的人是訪客的話，如果可以結合其他資料（如拜訪登記）知道是誰，一樣有可能是個資。

*圖片僅為示意圖

問25：如果監視器拍攝到特定人影像，這些影像是否為個資？

如拍攝到足以識別出特定個人之影像，無論是拍到當事人正面或鏡面、玻璃窗中反射影像，均為個人資料，需要依照《個人資料保護法》規定蒐集、處理、利用。

*圖片僅為示意圖

問26：影像中的身高或體態，是個資嗎?

廠商想要從監視影像中的身體特徵，透過大數據分析，進一步提供客製化服務

特徵

是否可直接/間接識別特定個人?

YES → 屬於個資

NO → 非屬個資，例如某群體的平均身高

參考條文：《個資法》第2條第1項

stli

31

2020 © 資訊工業策進會 Institute for Information Industry

問27：根據特徵資料分析出之人物屬性，是否為個資？

分析特徵資料後可以歸納出某些性別、年齡或體型的人可能具備之屬性，如男性或女性的平均身高。**上述人物屬性資料，如果沒有辦法回溯到特定個人身上，並非個人資料。**

如擷取十位兒童全身影像，蒐集到每位兒童身高、胖瘦等體型特徵，這些特徵資料為個人資料；進一步分析上述特徵資料，可以得知十位兒童平均身高和體重，但平均身高和體重等數字無法和和特定兒童連結在一起，故平均身高和體重並非個人資料。

stli

32

2020 © 資訊工業策進會 Institute for Information Industry

問28：監視器拍攝之人物動線是否為個資?

人物動線資料如為個人之行動履歷，可直接或間接識別出該個人，為個人資料。

問29：如果將動線轉為座標呢？

如進一步分析動線資料，將其轉化座標值，如2點50分（255，370），無法僅從數字識別出特定個人，則座標非個人資料。

stli

33

問30：門禁系統或監視器取得之個資，為一般資料還是特種資料?

門禁系統或監視攝影所拍攝的影像，一般而言不屬於上述6種「特種個資」，得為合理利用

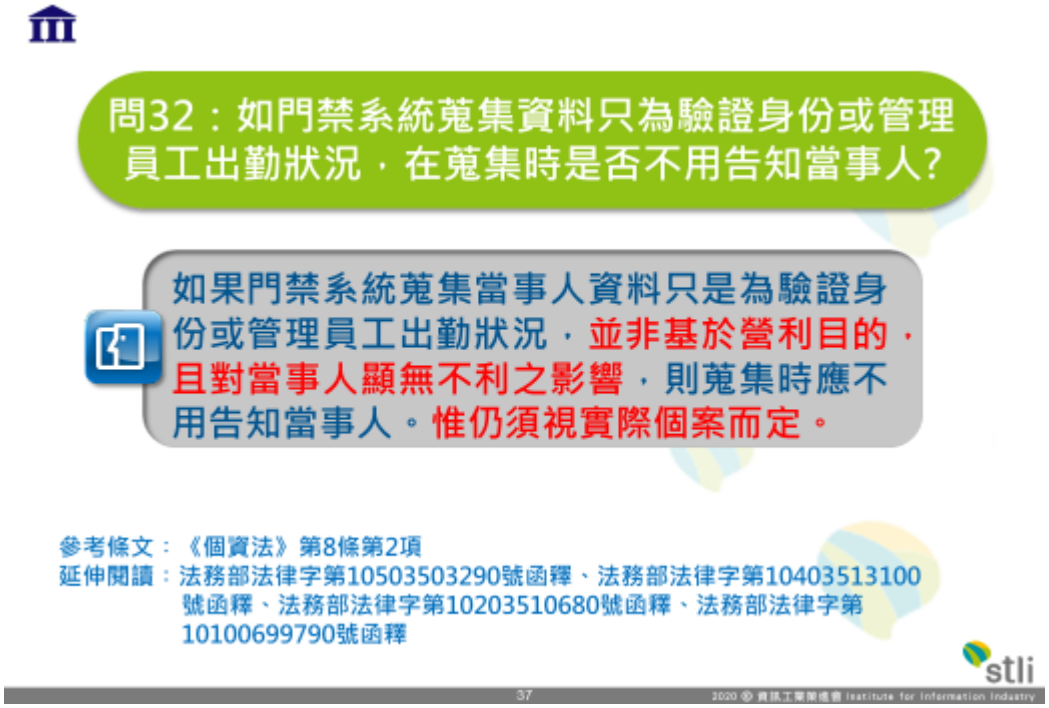
參考條文：《個資法》第6條第1項

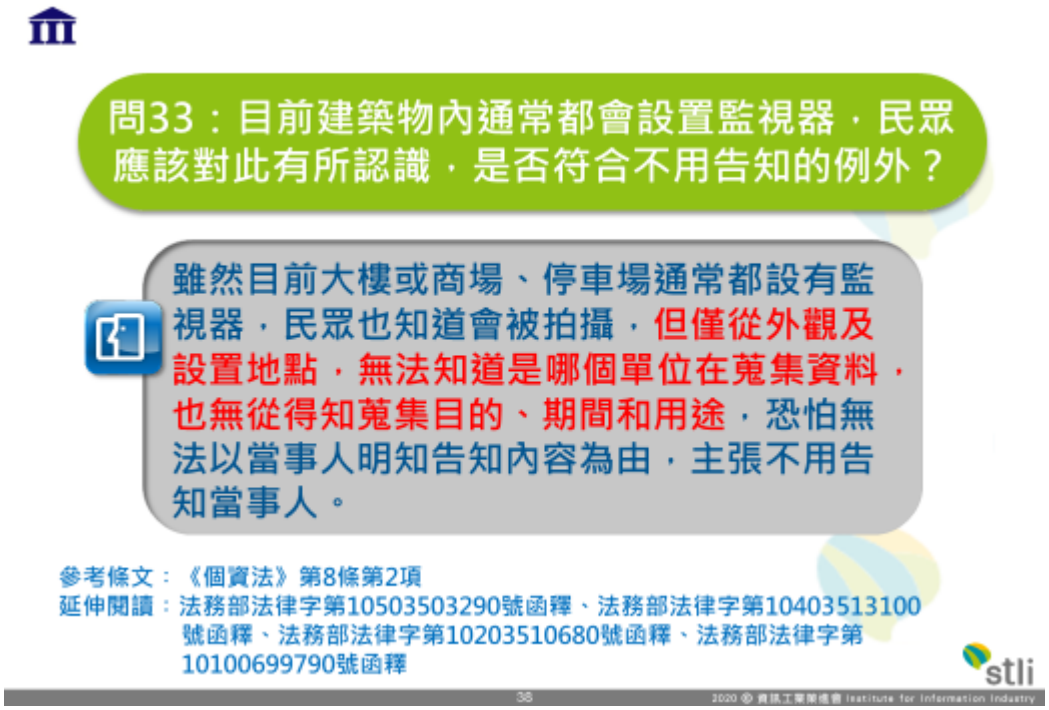
stli

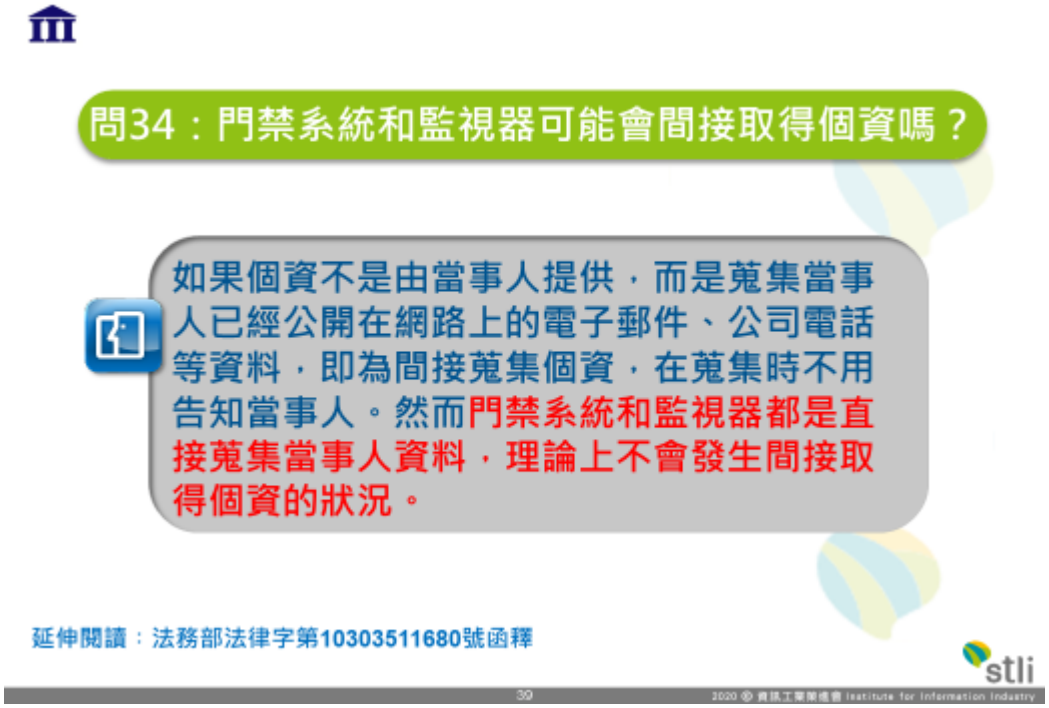
34

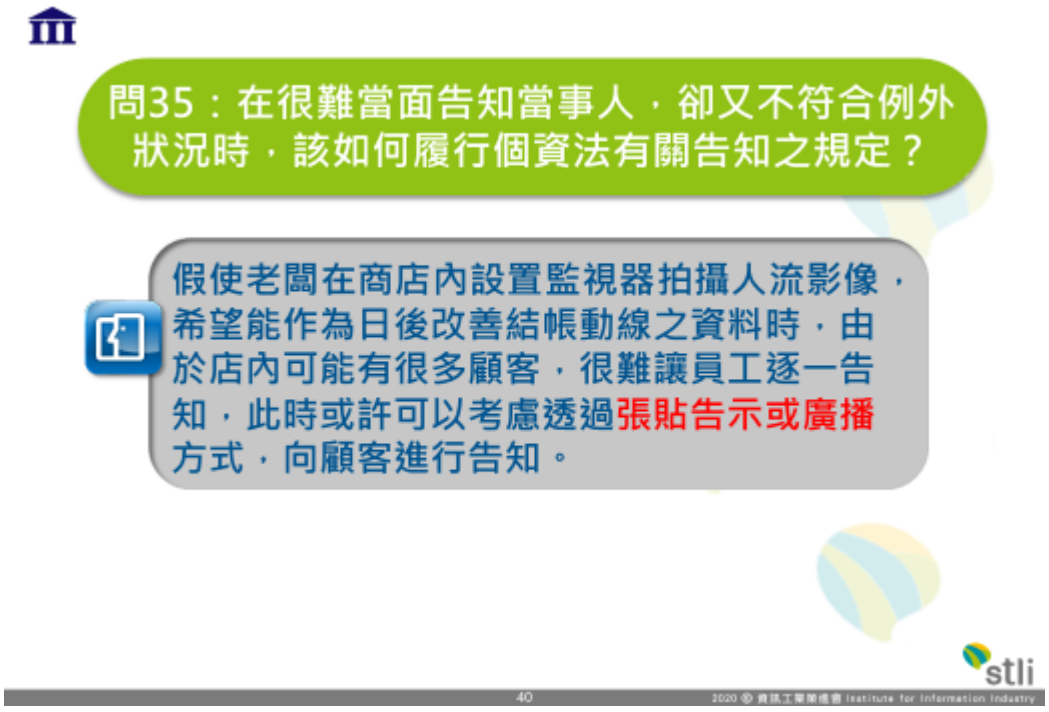

進階篇
蒐集資料時之注意事項
stli
35
2020 資訊工業策進會 Institute for Information Industry


問31：門禁系統或監視器蒐集資料時，可能遇到哪些問題?
門禁系統
如果是針對住戶或員工等蒐集資料，可以在蒐集前向當事人告知蒐集資料之目的、資料類別等事項。如果是針對訪客蒐集資料，很難當場向訪客清楚說明，或讓其理解告知的內容，可能就此產生糾紛。
安全監控設備
監視器可能因為設置地點較隱密、拍攝範圍較廣，或可能拍攝到不特定多數人等原因，使得在拍攝時很難告知當事人。即便透過張貼告示等方式進行告知，也無法確保所有人都會仔細閱讀告示或理解告示內容。
stli
36
2020 資訊工業策進會 Institute for Information Industry


問32：如門禁系統蒐集資料只為驗證身份或管理員工出勤狀況，在蒐集時是否不用告知當事人?
如果門禁系統蒐集當事人資料只是為驗證身份或管理員工出勤狀況，並非基於營利目的，且對當事人顯無不利之影響，則蒐集時應不用告知當事人。惟仍須視實際個案而定。
參考條文：《個資法》第8條第2項
延伸閱讀：法務部法律字第10503503290號函釋、法務部法律字第10403513100號函釋、法務部法律字第10203510680號函釋、法務部法律字第10100699790號函釋
stli
37


問33：目前建築物內通常都會設置監視器，民眾應該對此有所認識，是否符合不用告知的例外？
雖然目前大樓或商場、停車場通常都設有監視器，民眾也知道會被拍攝，但僅從外觀及設置地點，無法知道是哪個單位在蒐集資料，也無從得知蒐集目的、期間和用途，恐怕無法以當事人明知告知內容為由，主張不用告知當事人。
參考條文：《個資法》第8條第2項
延伸閱讀：法務部法律字第10503503290號函釋、法務部法律字第10403513100號函釋、法務部法律字第10203510680號函釋、法務部法律字第10100699790號函釋
stli
38


問34：門禁系統和監視器可能會間接取得個資嗎？
如果個資不是由當事人提供，而是蒐集當事人已經公開在網路上的電子郵件、公司電話等資料，即為間接蒐集個資，在蒐集時不用告知當事人。然而門禁系統和監視器都是直接蒐集當事人資料，理論上不會發生間接取得個資的狀況。
延伸閱讀：法務部法律字第10303511680號函釋
stli
39
2020 資訊工業策進會 Institute for Information Industry


問35：在很難當面告知當事人，卻又不符合例外狀況時，該如何履行個資法有關告知之規定？
假使老闆在商店內設置監視器拍攝人流影像，希望能作為日後改善結帳動線之資料時，由於店內可能有很多顧客，很難讓員工逐一告知，此時或許可以考慮透過張貼告示或廣播方式，向顧客進行告知。
stli
40
2020 資訊工業策進會 Institute for Information Industry

問36：門禁系統或監視器蒐集個資可能符合哪些特定目的？告知時需要說明個資類別，請問個資料有哪些類別？

關於可能符合之特定目的和個資類別，可上網搜尋「個人資料保護法之特定目的及個人資料之類別」參考。

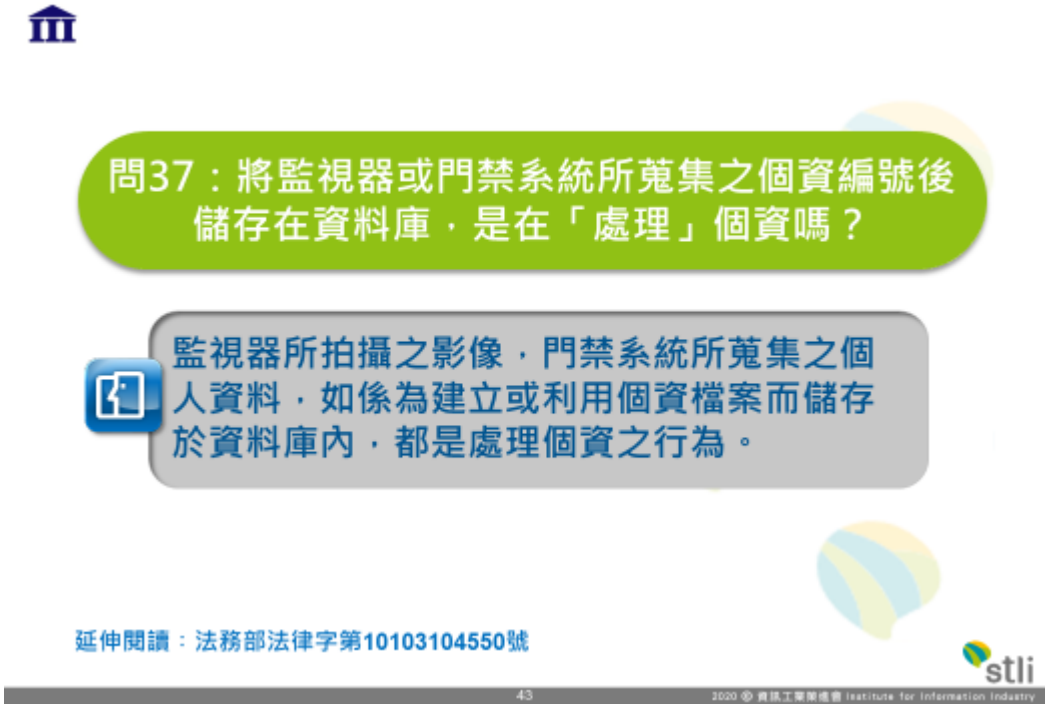
延伸閱讀：法務部法律字第10403505690號函釋

41

進階篇

處理資料時之注意事項

42


問37：將監視器或門禁系統所蒐集之個資編號後儲存在資料庫，是在「處理」個資嗎？
監視器所拍攝之影像，門禁系統所蒐集之個人資料，如係為建立或利用個資檔案而儲存於資料庫內，都是處理個資之行為。
延伸閱讀：法務部法律字第10103104550號
stli
43
2020 資訊工業策進會 Institute for Information Industry


問38：想要蒐集、處理個資亦可透過取得當事人同意方式為之，但怎樣算是表示同意呢？
表示同意之方式
蒐集、處理
當事人表示出允許之意思，就算不是非常明確的表示，只有點頭示意亦可。此外，就算當事人什麼都沒講，但如果沒有明確表示反對並已提供個人資料，也可認為已經同意。
利用
利用個人資料必須取得當事人明確的表示，不能只以當事人有點頭或沒表示反對為由，就認為對方已經同意我們利用其個人資料。
原則上不一定要以書面取得當事人同意，但如果是蒐集特種個資，就一定要取得書面同意。
stli
44
2020 資訊工業策進會 Institute for Information Industry

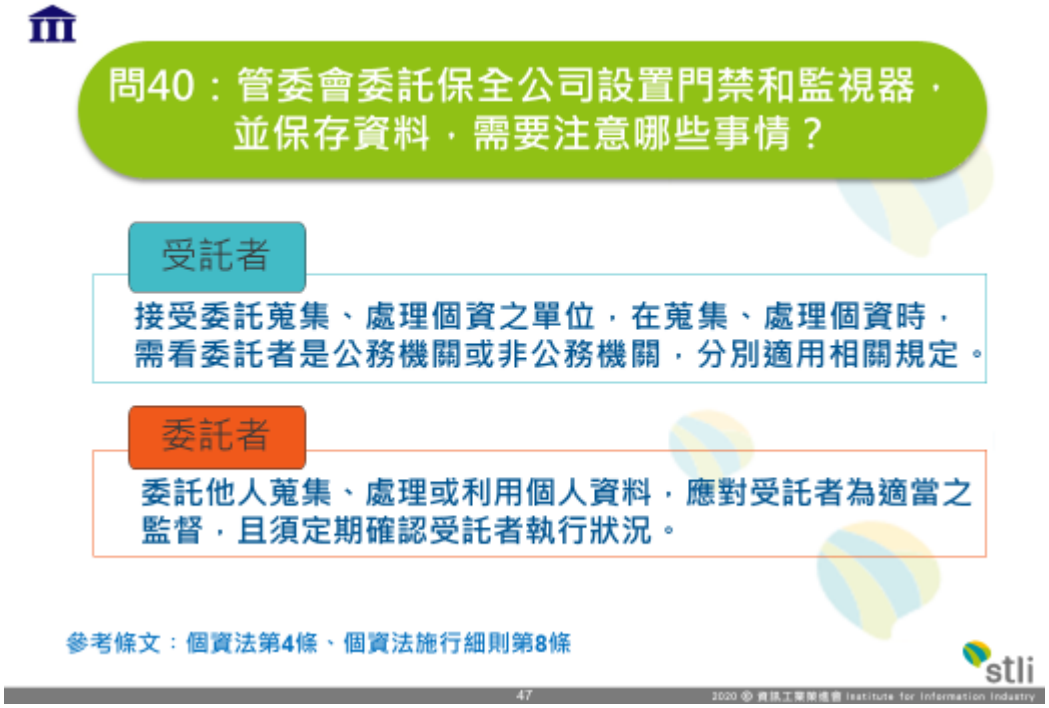
進階篇

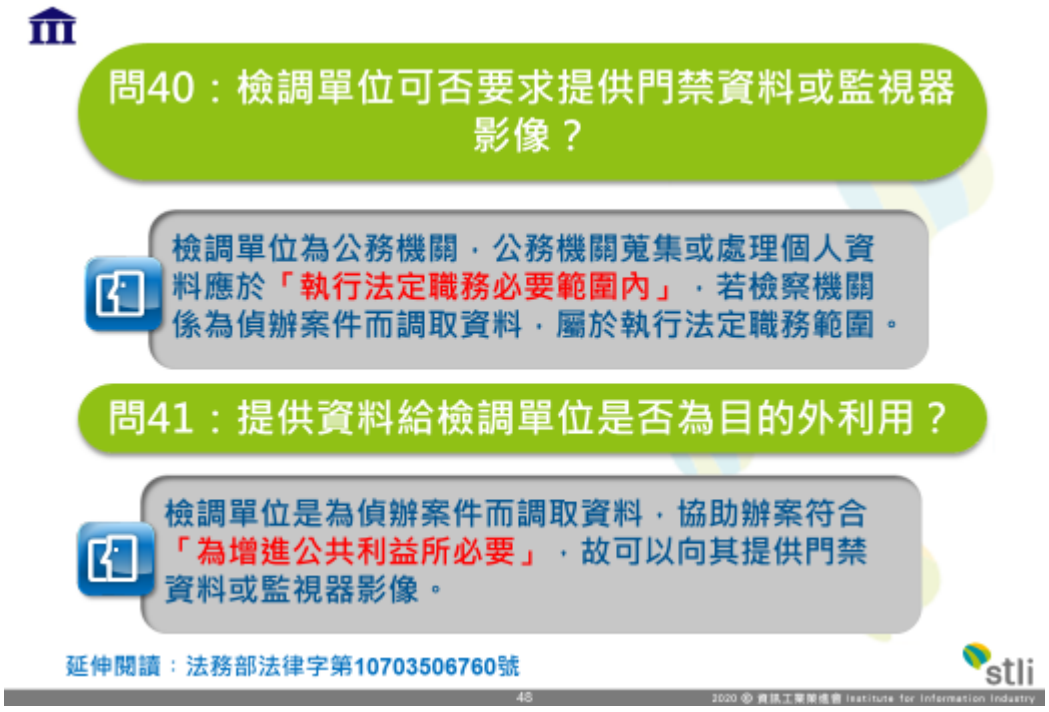
利用資料時之注意事項

問39：如果想要分析監視器所拍攝之影像，需要注意什麼地方？

個資法要求利用個人資料時，需要符合蒐集之目的，不能隨便將蒐集來的個人資料拿去做其他用途。不過為促進個資利用，個資法分別針對公務機關和非公務機關設有例外規定，想要利用個資者，可以檢查是否符合上述規定。

參考條文：個資法第16條、個資法第20條
延伸閱讀：法務部法律字第10503518090號、法務部法律字第10503512050號


問40：管委會委託保全公司設置門禁和監視器，並保存資料，需要注意哪些事情？
受託者
接受委託蒐集、處理個資之單位，在蒐集、處理個資時，需看委託者是公務機關或非公務機關，分別適用相關規定。
委託者
委託他人蒐集、處理或利用個人資料，應對受託者為適當之監督，且須定期確認受託者執行狀況。
參考條文：個資法第4條、個資法施行細則第8條
47


問40：檢調單位可否要求提供門禁資料或監視器影像？
檢調單位為公務機關，公務機關蒐集或處理個人資料應於「執行法定職務必要範圍內」，若檢察機關係為偵辦案件而調取資料，屬於執行法定職務範圍。
問41：提供資料給檢調單位是否為目的外利用？
檢調單位是為偵辦案件而調取資料，協助辦案符合「為增進公共利益所必要」，故可以向其提供門禁資料或監視器影像。
延伸閱讀：法務部法律字第10703506760號
48

問43：住戶可否要求管委會刪除或停止蒐集、處理、利用門禁系統或監視器保存之個資？

發生下列情況時，管委會應主動或依當事人要求停止蒐集、處理、利用個人資料，或刪除個人資料：

1. 個人資料蒐集之特定目的消失或期限屆滿時。
2. 違反個資法規定蒐集、處理或利用個人資料。
3. 當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者。

參考條文：個資法第11條第3項、個資法第11條第4項、個資法第19條第2項

案例篇

門禁系統

情境一：辦公大樓透過門禁系統紀錄員工進出時間和次數，管理出缺勤狀況

1 應用情境

	設置目的	設置區域	適用對象
門禁系統	出缺勤紀錄	辦公室門口	員工

2 蒐集資料

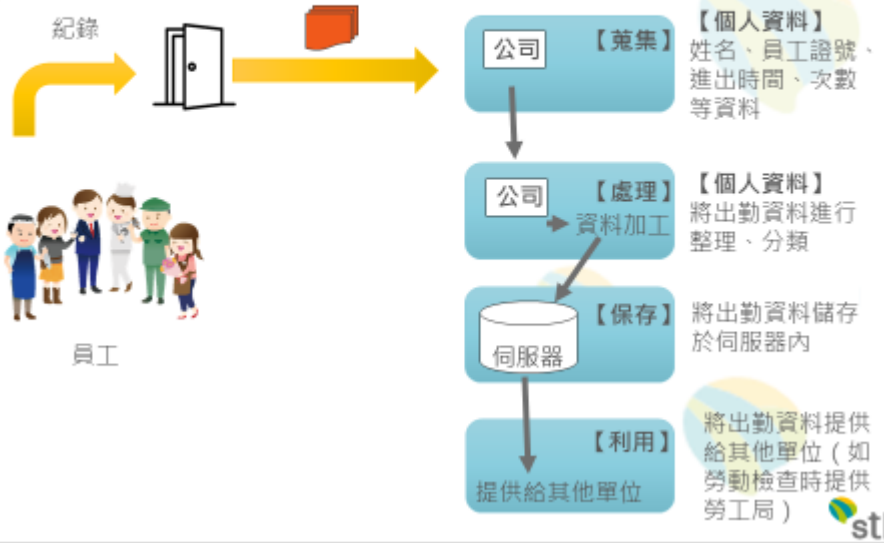
姓名、員工證號等身分識別資料。
進出門禁時間、次數等紀錄。

辦公大樓內裝設門禁系統，除管控人員進出外，通常還會紀錄進出時間和次數等資料，紀錄出缺勤狀況，故適用對象為員工。門禁系統所蒐集之資料通常為可用以辨別當事人身分之姓名、員工證號、進出時間、次數等資料，在整個資料應用流程中，可能遭遇的問題包括：姓名、員工證號等資料是否為個人資料，以及蒐集、處理、利用個資時是否需要告知當事人，以及是否符合特定目的和特定情形。資料應用流程和具體說明可參照下圖：

stli

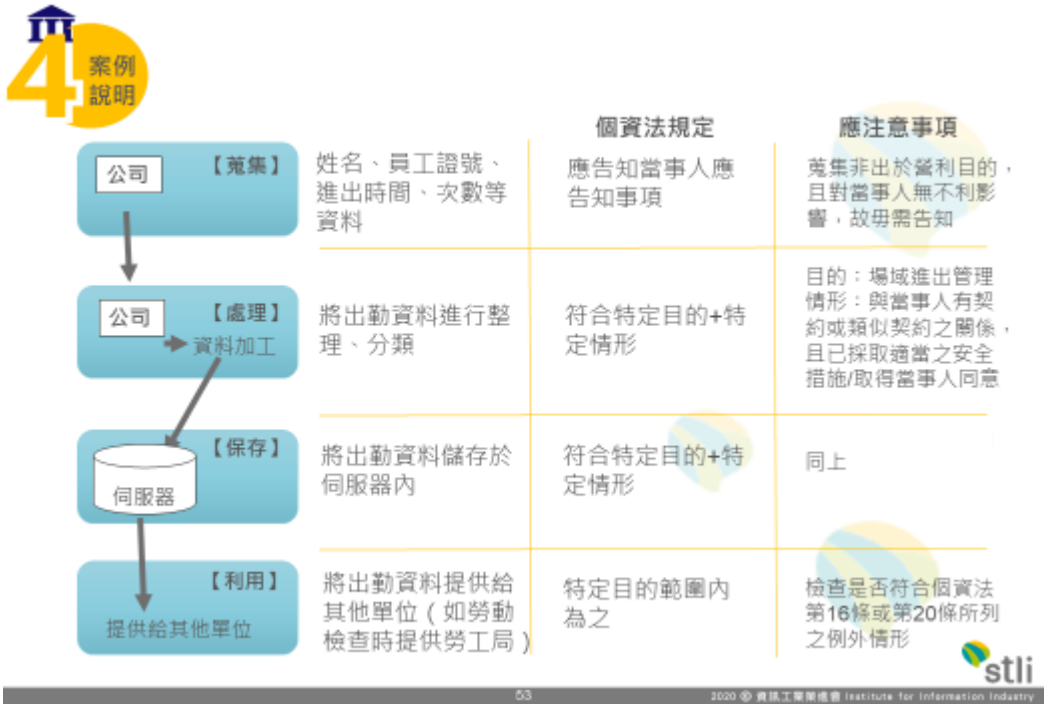
51 2020 資訊工業策進會 Institute for Information Industry

3 應用流程



stli

52 2020 資訊工業策進會 Institute for Information Industry


4
案例說明
個資法規定
應注意事項
公司
【蒐集】
姓名、員工證號、進出時間、次數等資料
應告知當事人應告知事項
蒐集非出於營利目的，且對當事人無不利影響，故毋需告知
公司
【處理】
資料加工
將出勤資料進行整理、分類
符合特定目的+特定情形
目的：場域進出管理情形；與當事人有契約或類似契約之關係，且已採取適當之安全措施/取得當事人同意
【保存】
伺服器
將出勤資料儲存於伺服器內
符合特定目的+特定情形
同上
【利用】
提供給其他單位
將出勤資料提供給其他單位（如勞動檢查時提供勞工局）
特定目的範圍內為之
檢查是否符合個資法第16條或第20條所列之例外情形
stli
53
2020 資訊工業策進會 Institute for Information Industry

參考書目

一、西文參考資料（依首字字母順序排列）

1. A National Surveillance Camera Strategy for England and Wales Executive Summary, Gov. UK, https://www.gov.uk/government/publications/national-surveillance-camera-strategy-for-england-and-wales.
2. European Data Protection Supervisor, Guidelines on the protection of personal data in IT governance and IT management of EU institutions, 2018/03/23, https://edps.europa.eu/data-protection/our-work/publications/guidelines/it-governance-and-it-management_en.
3. European Data Protection Board, Guidelines 3/2019 on processing of personal data through video device, 2020/01/30, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.
4. Information Commissioner's Office[ICO], Surveillance Camera Code of PracticeJune (2013).
5. Information Commissioner's Office[ICO], In the picture: A data protection code of practice for surveillance cameras and personal information(2017).
6. Xu Zheng, Zhipeng Cai, and Yingshu Li, Data Linkage in Smart Internet of Things Systems: A Consideration from a Privacy Perspective, IEEE Communications Magazine, Volume56, Issue 9(2018).

二、日文參考資料（依首字筆畫順序排列）

1. IoT 推進コンソーシアム、総務省、経済産業省，《カメラ画像利活用ガイドブック ver2.0》，2018。
2. ZDNet Japan，〈IoT や AI に対して不安「個人特定」「情報漏えい」--忘れられる権利を希望-日立調査〉，https://japan.zdnet.com/article/35094097/。
3. ZDNet Japan，〈IoT のセキュリティに不安を感じる企業は半数以上 -ForeScout の調査結果〉，https://japan.zdnet.com/article/35110195/。
4. 〈カメラ画像利活用ガイドブック ver2.0」を策定しました〉，経済産業省，https://www.meti.go.jp/press/2017/03/20180330005/20180330005.html。
5. 内閣サイバーセキュリティセンター，〈サイバーセキュリティ関係法令 Q&A ハンドブック作成・公開のお知らせ〉，2020/03/02，https://www.nisc.go.jp/security-site/files/lawhandbook_press.pdf。
6. 内閣サイバーセキュリティセンター，《サイバーセキュリティ関係法令 Q&A ハンドブック》，2020。
7. 《個人情報保護を巡る国内外の動向》，2018，https://www.ppc.go.jp/aboutus/minutes/2018/20190320/。

8. 〈個人データに利用停止権、改正個人情報保護法が成立〉，日本經濟新聞，2020/06/05，https://www.nikkei.com/article/DGXMZO60009640V00C20A6MM0000/。
9. 個人情報保護委員会，〈「個人情報の保護に関する法律等の一部を改正する法律案」の閣議決定〉，2020/03/10，https://www.ppc.go.jp/news/press/2019/20200310/。

三、中文參考資料

1. 王明德，〈建構智慧建築系統延伸基本功能擴大市場〉，《SmartAuyo》，2018。
2. 王岫晨，〈智慧建築趨勢：綠能、感測與互聯〉，《CTIMES》，2014。
3. 台北市政府，《台北市政府公共住宅智慧社區建置參考手冊》，2018。
4. 內政部營建署，《智慧建築設計技術參考規範》，2012。
5. 李世德，〈GDPR 與我國個人資料保護法之比較分析〉，《台灣經濟論衡》，第 16 卷第 3 期，2018。
6. 周晨蕙，〈產業資料與個人資料之加值運用法制-以日本為例〉，《科技法律透析》，第 31 卷第 9 期（2019）。
7. 施弘文，〈歐盟執委會提出「隱私與電子通訊規則」草案〉，《科技法律透析》，第 29 卷第 6 期，2017。
8. 徐彪豪，〈物聯網時代的資料保護防線－以歐盟 GDPR 為中心〉，《科技法律透析》，第 28 卷第 10 期，2016。
9. 葉志良，〈因應物聯網發展資料保護法制的革新-歐盟法制的發展與啟示〉，《中原財經法學》，第 40 期，2018。

四、網路資料

1. 〈推動開放資料專法 建構資料共享新世代〉，國家發展委員會，https://www.ndc.gov.tw/News_Content.aspx?n=114AAE178CD95D4C&sms=DF717169EA26F1A3&s=0E2ADAF00CD83B6B（最後瀏覽日期：2020/09/29）。
2. 〈爭取歐盟 GDPR 適足性認定 國發會：去年底已遞件〉，自由時報，2019/02/18，https://ec.ltn.com.tw/article/breakingnews/2702576（最後瀏覽日：2020/09/22）。
3. 國家發展委員會，〈歐盟 GDPR 與我國個人資料保護法之重點比較分析〉，https://www.ndc.gov.tw/Content_List.aspx?n=92A54D2FBC1D329E（最後瀏覽日期：2020/10/06）。