「歐盟國家個人資料保護法制因應 GDPR 施行之調適-以德國與英國為例」委託研究計畫

結案報告

委託單位：國家發展委員會

受託單位：世新大學

中華民國 109 年 5 月

「歐盟國家個人資料保護法制因應 GDPR 施行之調適-以德國與英國為例」委託研究計畫

結案報告

受委託單位：世新大學

研究主持人：翁逸泓

協同主持人：李寧修

研究期程：中華民國 108 年 5 月至 109 年 5 月

研究經費：新臺幣 95 萬元

國家發展委員會 委託研究

中華民國 109 年 5 月

摘要

本報告之目的係針對歐盟會員國如何落實 GDPR 之情形加以觀察並分析，本報告分別對德國聯邦個人資料保護法與英國 2018 年資料保護法之內容及二國各自落實 GDPR 之實際情形提出說明，且另就擇定之我國目前較急迫或具有重要性之議題分析英國、德國與我國個資法之異同。這幾個議題分別是監管機關之中央與地方權限、個資特定目的外利用之要件、去識別化之要件、程序、認定方式等規定、特殊處理情形(GDPR 第 9 章)、自動化機器做成之決策，以及當事人權利之議題相關的法律制定與政策落實等。

本報告認為我國在法制上如要完善個資保護法制，甚至企圖實現良好的資訊治理，實有必要將法制更加以完備。而一個獨立專責且能量充足的監管機關，是推動個資保護法制的必要機構性之保護架構。對此，最基本的關鍵在於本報告所分析的所有相關爭點，都需要仰賴這個專責機關依照其所被賦予的職權，例如教育宣導、法令解釋、監督管理、執法制裁等各方面具有充分能量的行政作為，來實現個資法制上對於當事人權利之保護，以及對於資料控管者義務之監督。

此外，目前個資法缺乏利益衡量之條款，也使得僵化而機械的文義解釋經常被提出，令社會產生對於個資保護法制之疑懼，擔心其落實會限制數位科技之應用，而紛紛希望以去識別化之方式脫離個資法範圍，又或期待創設各種例外豁免（特種）個資保護之規範，更任意依照主觀心證解釋所謂「公共利益」之範圍與內涵。

最後，在追求至少跟得上 GDPR 腳步而落實相關法制的同時，或許面對我國對數位經濟發展政策的渴望，在個資保護法制上對包括人工智慧（機器自動化）決策、通訊傳播與健康研究應用等不同領域上，可以考慮「超前部署」，以其作為我國資訊治理政策的起點。

Abstract

This report aims to observe and analyze how EU member states implement GDPR. This report provides explanations on the content of the The German Bundesdatenschutzgesetz (BDSG) and the 2018 Data Protection Act of the United Kingdom, as well as the implementation of the GDPR in the two countries. The report also analyzes the similarities and differences between the UK, Germany and Taiwan personal data protection laws on selected issues that are more urgent or important in Taiwan. These issues are the supervisory authority, the requirements for the use beyond the scope of the purposes for which the personal data was collected, the requirements for de-identification, provisions relating to specific processing situations, and automated individual decision-making, and legal formulation and policy implementation related to the rights of data subjects.

This report considers that, firstly, it is necessary to make the Taiwanese legal system more complete to improve the legal system of personal data protection, or even attempt to achieve good information governance. To do so, an independent, dedicated and capable supervisory authority is an essential institutional framework to promote the legal system for personal data protection. In this regard, the most fundamental point is that all the relevant disputes analyzed in this report need to rely on the agency in accordance with its assigned powers, such as education and publicity, legal interpretation, supervision and management, law enforcement sanctions and other aspects. Moreover, this can lead to proper realisation of the protection of the rights of data subjects and the supervision of the obligations of data controllers in data protection legal regime.

Secondly, the current lack of rights-balancing clauses in personal data protection law also makes rigid and mechanical literal interpretations often proposed, causing the society to have doubts and fears about the legal system for personal data protection, worrying that its implementation will limit the application of digital technology. This misinterpretation leads to wrongs that the method of identification is out of the scope of the personal data protection law, or it is expected to create a variety of exceptions and exemptions (special categories) of the protection of personal data, and

arbitrarily explain the scope and connotation of the so-called ‘public interest’ based on subjective evidence.

Finally, while pursuing at least keeping up with the GDPR and implementing relevant legal systems, perhaps facing Taiwan desire for digital economic development policies, the legal system for personal data protection in different fields such as applications of artificial intelligence (machine automation) decision-making, communication and health research, ‘advance deployment’ can be considered as the starting point of the government information governance policy.

目錄

第一章　前言

在 2016 年後，我國在數位經濟面向以「發展活躍網路社會、推進高值創新經濟、建構富裕數位國家」做為政策所欲達成之願景。而在政策宣示的網路社會環節中，則表示「保障數位人權，發展活躍網路社會」係政府之重要政策目標[1]。再者，在 2016 年的第十次全國科學技術會議總結報告[2]中，數位經濟與資料科技之加值應用及相關的隱私問題更是屢見其重要性。例如，在該次全國科技會議的第一個議題「創新再造經濟動能」中，主要策略例如「創新數據服務，活化跨域資料應用」之措施[3]，即開宗明義明白地宣示性地認為「打造兼顧個人隱私與產業發展之跨域資料整合應用環境，以創造資料經濟價值」係完成「創新產業的數位經濟發展模式」遠景的第一要務[4]。此時，論及所謂的「數位經濟」，則當然「數位化(digitalisation)」必然會是最關鍵的一個步驟；而「數位化」之後，第一個立即產生物便是數位化生成之「資料(data)」。對於該等資料之加值應用，便延伸出當前臺灣街頭巷議乃至於政府、各研究單位與通訊傳播、平面媒體等觸及圍繞的幾個新興科技話題：巨量資料、智慧聯網、雲端運算、OTT(Over-The-TOP)、行動支付與

---

[1] 行政院(新聞傳播處),《林揆:推動數位國家.創新經濟發展方案 促進數位經濟與環境》，2016 年 11 月 24 日，http://www.ey.gov.tw/News_Content2.aspx?n=F8BAEBE9491FC830&sms=99606AC2FCD53A3A&s=1C4972D063F7B02B，（最後瀏覽日期：2019 年 4 月 10 日）。

[2] 科技部，《第十次全國科學技術會議總結報告》，2016 年 12 月 13 日，http://2016technology.tw/images/nsf_pdf/final/10th-report.pdf，（最後瀏覽日期：2019 年 4 月 10 日）。

[3] 其具體措施包括有：
(1) 建構跨域資料交換標準與服務平台；
(2) 帶動跨域資料創新服務合作網絡；
(3) 推動跨域實務數據人才培訓；
(4) 完備資料服務產業供應鏈；
(5) 發展特色領域產業資料應用。
參：前揭註，頁 3。

[4] 前揭註，頁 2。

開放（政府）資料以及邇近熱門的人工智慧與機器學習等。

另一方面，個人資料之蒐集、留存、處理與利用透過巨量資料科技手段之應用不惟發生於國際上，臺灣藉由推動政府機關所持有巨量資料之應用研究，深化電子化政府應用之情況，亦已然實際發生。例如，行政院在其所通過關於第五階段電子化政府計畫之核定本中，願景在於運用雲端與物聯網巨量資料特性，以資料導向之角度重新設計政府服務樣態，打造領先全球的數位政府[5]。綜觀掌握全球資訊環境發展脈絡，依「生活新型態」、「經濟新應用」與「治理新模式」三大層面，概述資通訊科技未來之發展預測。其中在「生活新型態」的面向中提及民眾生活逐步數位聯網化，例如巨量資料分析與穿戴式設備將加速實現遠距醫療與照護[6]；而在數位經濟層面，該計畫提及政府各機關當妥善地「運用數位資源，並且搭配法規調適，協助企業資訊化、知識化、智能化，翻轉經營服務模式，創造產業新價值。各機關將以數位化及標準化之資料介接方式，簡化民間及企業對政府申辦流程，促進企業運作模式創新。並以巨量資料，提供有效之產業相關預測，以提升民間服務建置之經濟效益[7]。」

行政院於 2018 年 5 月 24 日院會責成國家發展委員會儘速成立「個人資料保護專案辦公室」，辦公室已於 2018 年 7 月 4 日正式運作，二大工作重點之一厥為向 GDPR 取得歐盟之適足性認定(adequacy decision)。這是由於 GDPR 的域外效力規

[5] 國家發展委員會，《第五階段電子化政府計畫 – 數位政府核定本（106-109 年）》，2016 年 1 月，http://www.ndc.gov.tw/cp.aspx?n=67F4A482298C5D8E&s=EEBA8192E3AA2670，最後瀏覽日期：2019 年 4 月 10 日，頁 17。

[6] 國家發展委員會，《第五階段電子化政府計畫 – 數位政府核定本（106-109 年）》，頁 2。

[7] 國家發展委員會，《第五階段電子化政府計畫 – 數位政府核定本（106-109 年）》，頁 18。

定擴張其適用，使得非歐盟境內的資料控管者(data controller)及受託處理者(processor)也可能受其拘束，在未有前述適足性認定之狀態下，歐盟域外之企業等如希冀與世界最大之經濟體歐盟交換個資，則需自行承擔採行標準個資保護契約條款(SCC)、拘束性企業規則(BCR)、行為守則(CoC)及認證(Certification)等四種國際傳輸方式，或基於當事人明確同意、符合因執行契約所必要、基於公共利益之重要原因，以及於當事人無法為同意之表示時，移轉對其有重要利益保護必要等例外情形。因此我國相關機關為促進產業發展，節省個別產業法遵成本並避免法律風險，積極推動適足性認定。

最後，「108 年國家發展計畫－衝刺建設貫徹執行力」已於 2018 年 12 月 20 日行政院第 3631 次會議通過，並奉行政院 2018 年 12 月 27 日院臺經字第 1070045829 號函核定，分行各機關積極推動辦理。該計畫其中關於「發展數位經濟」之環節，即包含有「推動 GDPR 適足性認定」，並列為重要政策[8]。從而，對於 GDPR 之國際性比較法上之關懷與在地化之研究，至為重要。

雖然對於 GDPR 內涵與應用之介紹與研究於臺灣近年之文獻與研討活動相當踴躍與熱切，但是一個相對較為完整的 GDPR 如何施行於一個準據法體系中，以及在實際執行層面上如何將其化為簡單文字的規範具體落實，在中央與地方政府及各部會業管不同性質個資等行政措施之銜接等，則較少有著墨。這是因為事實上 GDPR 固然在一定之程度上或許可以被認為稍微嚴格，然而，臺灣的個資法就法條而論其實亦有一定水準

[8] 國家發展委員會，《108 年國家發展計畫－衝刺建設貫徹執行力》，https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC8xMjIxNi8zNzRkNzAyZS1mMTliLTQxMzMtOGYxZi1jMDAwNWFmMTFkZjYucGRm&n=MTA45bm05ZyL5a6255m85bGV6KiI55WrKOeyvue%2bjuacrCkt5YWo5pu4KOW9qeiJsuWwgemdoikucGRm&icon=..pdf ，最後瀏覽日期：2019 年 4 月 10 日，頁 13。

之保護；究其問題，在於臺灣之個資法權責分散，並未落實。

基於此，本研究計畫目的在處理前述需求，觀察、研究並分析當前對於個人資料相關權利保護最嚴謹的歐盟「一般資料保護規則(General Data Protection Regulation, GDPR)[9]」在歐盟會員國之施行(implementation)，包含了法制與實際之執行狀態。為此，分別研究德國聯邦個人資料保護法與英國 2018 年資料保護法(Data Protection Act 2018, DPA 2018)之內容及二國各自落實 GDPR 之實際情形，且另就擇定之我國目前較急迫或具有重要性之議題分析英國、德國與我國個資法之異同。

本報告採取文獻研究法，以德國及英國兩個分屬歐陸法系與英美法系典型之歐盟會員國之國內法律制度及執行狀況作為比較上之參照基準，除觀察歐盟之會員國如何落實並施行如此嚴謹之個資權利保護法制，尤其是較原有指令之更新部分，如當事人（權利主體）更為強化之個資近用權利，如可攜權與被遺忘權等，以及相對資料控管者之課責(accountability)及相關適足性(compliance)認定之義務要求，並大幅提高相對應罰則等，在會員國中如何地被聚焦與落實。

另外，本報告並針對目前國際間以及臺灣本身對於個人資料加值應用之熱門議題，如「去識別化/ 匿名化/ 假名化」之要件、程序、認定方式等規定、監管機關之中央與地方權限、自動化機器做成之決定以及包括兒童行使權利之議題等，提出觀察與分析。最後，並提出臺灣如希冀爭取歐盟之適足性認定，所可能之方向指引。

在架構上，本報告先分別介紹英國與德國各自在監管機關之中央與地方權限；個資特定目的外利用之要件；去識別化之要件、程序、

[9] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

認定方式等規定；特殊處理情形(GDPR 第 9 章)；自動化機器做成之決策；以及當事人權利之議題相關的法律制定與政策落實。其後，將該等分析與我國現況相較，提出建議。又，基於將對於 GDPR 之對應部分先行分析後，再為會員國法制落實與實踐之分析介紹較符合論證邏輯，因此本報告於分析英國之部分，依照分析主體之順序，將先分析 GDPR 有關之爭點。

第二章　英國個人資料保護法制介析及落實 GDPR 之實務狀況

第一節　法制沿革

英國雖有脫歐議題，但是關於個資保護之制度，其資訊委員(Information Commissioner, IC)亦明言英國之個資保護法制與執行基於 DPA 2018 之立法，不會受到干擾與變化。這是因為英國的 DPA 2018 幾乎是 GDPR 之複製版本，也因此即便英國脫歐，也能盡量避免有個資保護之法制落差與銜接問題。英國脫歐之真正問題在於關於國際傳輸方面，也因此在適足性認定上，英國在脫歐前的準備必須十分地充分，這也正是為何臺灣如要爭取歐盟適足性認定，必須觀察英國之狀況：一個從體制內(insider)變成體制外(outsider)的過程，展現出適足性認定最迫切之重要與實際操作。以英國為例，該國為施行資料保護指令，除 1998 年人權法(Human Right Act, HRA)落實人權保障外，亦有 1998 年資料保護法(Data Protection Act 1998, DPA 1998) [10]。基於保障個資之基本核心原則並無太大變化，因此現任英國資訊委員 Elizabeth Denham 指出雖然 GDPR 為英國之個資保護帶來重大改變，但是事實上並未改變「所有」之機制，與其將 GDPR 視為革命(revolution)，毋寧將其視為是個資保護機制的一種進化(evolution)，因此「理當」（畢竟，GDPR 之立法歷經四年，更有兩年之日出調適期）對於 GDPR 及早調適的英國企業來說，其陣痛感應當不至於太嚴重。

以英國 DPA 2018 之架構與內容言，如前所述，大致上與 GDPR 規範一致以減少未來脫歐之法規陣痛機會成本：主要之部分在架構如何落實 GDPR 的個人資料處理原則、法律執行等。此外，在授與會員國可彈性立法之部分，另包含有四個主要部分：GDPR 之補充、於特殊案件之調整、法律執行機關以及國安情報之例外等。

[10] 須注意者，英國在 1984 年便制定資料保護法(Data Protection Act 1984)，並成立資料保護登記官(Data Protection Registrar)，此即為英國資訊委員辦公室(ICO)之前身。

在實際負責英國國內對於 GDPR 之執行層面上來說，需特別注意明確區分兩個不同機關之職責：

1. 政府部門確保 GDPR 於英國要求之適足性的部會係為英國文化、媒體與運動部(Department for Digital, Culture, Media and Sport, DCMS)，且 DCMS 也負責制定英國資料保護法之立法，但並不執行 DPA 2018 之實際施行；
2. 相對地，英國資訊委員辦公室(The Information Commissioner's Office, ICO)職責之一即在落實執行 GDPR，其權力包括（關於個資）犯罪調查與罰鍰等，並提供企業與人民團體與政府機關（包含地方政府）對於如何適應 GDPR 之指引。

為因應 GDPR 與 DPA 2018 之變動，ICO 亦對應相關執行作為。在針對法制落實之執行面向上，即便在 DPA 2018 施行前，ICO 也一向對於政府機關以及私人團體採取不同之策略[11]：

1. 對於政府機關，ICO 著重於持續審查對於其執掌之相關法規範與政府之相關程序作為，確保政府在處理相關個資時，均依循資料保護法所揭櫫之原則，並盡到相關之資料控管者責任。如民眾對於政府機關之作為向資訊委員申訴者，ICO 並會釋出相關之訊息以及相對應之指導方針並將之公開化。
2. 對於私部門，則是強化民間組織之通知程序與相關之資料控管者登記作業。
3. 此外，ICO 也希望能夠在未來爭取到更多的人事配置資源俾利處理相關事務，並且能在機關嚴重違反資料保護以及資訊公開義務時，對於資訊委員之決定，能具更有效之拘束力[12]。而這個期待，也在

[11] 詳參：翁逸泓、廖福特，私生活權利：探索歐洲，反思台灣，台北：新學林出版，2014 年 12 月，頁 277-278。

[12] ICO, Corporate Plan 2008-2011. Retrieved October 5, 2009, from http://www.ico.gov.uk/upload/documents/corporate_plan_html/corpplan/enforcing.html.

英國政府的支持之下，讓英國的專責機關成為國際上編制最齊全的機關，並進而成就相關能量。

在 ICO 於 2018-2019 年度報告當中[13]，特別針對落實執行 GDPR 與 DPA 2018 而獨立一個章節專門說明與分析。這個說明的章節在架構上區分為「支持公眾」、「支持個資保護長(Data Protection Officer, DPO)」、「支持中小企業(SMEs)」、「協助組織內化 GDPR 與 DPA 2018」、「起草法規」等實際執行措施，而這些重點措施，也在一定程度上足以作為我國未來希冀調整個資法後，如果有專責個資機關時的借鏡。

1. 對公眾之支持

在此一部分 ICO 主要將注意力集中在喚醒公眾的隱私與個資保護意識，在 2018 年中，ICO 的調查顯示約有三分之一的民眾或組織對於其個資利用有高度信任與信心。其中一項最大的關鍵點在於大多數民眾乃係透過 ICO 發行之宣導刊物，包含 GDPR 指引以及個資自我檢視工具說明等，進而強化隱私意識[14]。

2. 對 DPO 之支持

ICO 認為 GDPR 與 DPA 2018 對 DPO 賦予重要之責任，尤其是在新的個資保護規範架構下，DPO 對於促使各機構組織快速適應新法，有著重要角色。

據此，ICO 每年均針對 DPO 召開實踐個資保護政策的研討會，並頒發相關獎項鼓勵傑出 DPO，也趁機對其宣達政策[15]。

3. 對中小企業(SMEs) 之支持

[13] ICO, Information Commissioner's Annual Report and Financial Statements 2018-19, https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.
[14] Ibid., 16.
[15] Ibid., 18.

除了前述有 DPO 的組織以外，ICO 也充分理解小型組織要符合 GDPR 和 DPA 2018 並非易事，尤其是對於個體交易者而言，更顯其困難。為此，ICO 提供了一套資源、支持和指南，專門針對個體交易者和小型組織的需求，包括可能的操作選項和清單，社群媒體平台和常見問題解答。ICO 也對此提供了專門的求助熱線和即時聊天服務，以提供進一步的幫助和建議，並舉行由數百家中小企業參加的諮詢會議。

除了這些服務以外，ICO 目前正在探索為中小企業建立「一站式服務」，以匯集各個監管團隊的專業知識來幫助 ICO 為所有中小企業提供支持，尤其是對於那些沒有能力維護專用內部合規資源的中小企業[16]。

4. 協助組織內化 GDPR 與 DPA 2018

在 2018-19 年度觀察期間，ICO 具體制定了全面性的 GDPR 指引，以幫助私部門組織將 GDPR 和 DPA 2018 內化至日常工作中。其後增加重要內容，包括契約（範本）、DPA 豁免和加密等領域，也提供了一個互動應用程式作為工具，以幫助其了解合法的個資處理基礎。而這個指引在 2018-19 年度期間已被世界各地的組織廣泛使用，最適切的證明就是在 2018-19 年度，該指引在 ICO 網站上的瀏覽量超過 1500 萬次。最後，ICO 也持續開發溝通的互動應用程式工具以及相關的法規說明指引與宣導文件，並已獲得歐盟個人資料保護委員會（European Data Protection Board, EDPB）之良好反饋[17]。

5. 起草法規

在 2019-20 年間，ICO 提供根據 DPA 2018 必須制定的四項法定守則（將在本報告詳述）。這些守則將重點聚焦在包括適合年齡的設

[16] Ibid., 19.
[17] Ibid.

計、資料共享、行銷以及個資保護和新聞自由，另外，ICO 也發表在政治競選時利用個資的指引等[18]。

綜合來說，英國資訊委員在具體深化新法規調適的工作上，較明顯地把重心放在宣導、發布相關指引、發布法規命令等，而本報告認為最重要的訣竅在於針對不同需求群體，做出分層分流，目標導向的行動，以符合各自的不同需求。其次，有效善用 DPO 作為 ICO 與民眾及私人組織的連結，也有其效率性。

而之所以能具體地顯示出調適新法規的效率性，ICO 事實上在 2018-19 度新增投入相當地顯著。依據 2018-19 年度報告，該年度是 ICO 顯著擴張的一年：其人員配備水平在這一年增加了將近 200 名員工，ICO 辦公處所所在地的威爾姆斯洛（Wilmslow）主要住房的佔地面積，也擴大了 79%，以跟上其不斷擴張的人員編制[19]。

第二節　英國個人資料保護之法制框架與特色

一、 監管機關之中央與地方權限

(一) 中央監管機關：資訊委員(Information Commissioner) [20]，一個獨立集中專責個資保護的機關

GDPR 第 51 條以下規範承繼原本歐盟資料保護指令要求的會員國設立獨立監管機關措施，以作為機構性之保護架構(institutional framework)，要求各會員國應設立至少一個獨立公務機關職司 GDPR 適用之監控，以保護當事人有關個人資料處理之基本權與自由及促進

[18] Ibid., 20-22.
[19] Ibid., 64.
[20] 因為本報告此部分並非專為討論中央監管機關即 ICO，而係處理中央與地方監管機關之權限分配問題，因此僅就關聯部分說明。關於英國資訊委員權責在規範上之詳細介紹，參：達文西個資暨高科技法律事務所，國家發展委員會 106 年度「個人資料保護專責機關與資料在地化之法制研究」委託研究計畫結案報告，國家發展委員會，2018 年 05 月 15 日，頁 39-59。

歐盟內部個人資料之自由流動。如果會員國設置了一個以上之監管機關，則同條第 3 項規範有該會員國應「指定其一於委員會代表各監管機關，並應建立機制，以確保其他機關遵循與第 63 條所稱之一致性機制有關之規範」，因此就 GDPR 而言，對於個資保護之監督管理專責機關之組織建立模式，應可推定為較鼓勵會員國採取集中式之型態，而指定唯一機關代表該會員國。再者，GDPR 第 52 條特別強調該等監管機關之獨立性，並在第 1 項明示授與各會員國個人資料保護監督機關獨立性之正當性，且其獨立性應受保障之程度，可從下列四個面向窺見：

1. 地位：至少需達到不受直接或間接之外部干擾、不依循任何人之指揮、不得為與職務衝突之行為、無論報酬不得兼職[21]；
2. 設施：該中央監管機關具備有效行使職權所需之人力、技術及財務資源、辦公室以及各項基礎設施[22]；
3. 人事：監管機關應可自行選擇並擁有自身之人員，且渠等人員應受該監管機關成員排他之指示，以及各項透明任命程序與任期之保障[23]；與
4. 財務預算：各監管機關雖應受財務控制，但不得影響其獨立性，且其應有單獨、公開之年度預算，並得作為國家或聯邦整體預算之一部分[24]。

[21] Art. 52 (2): …in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody; and Art. 52 (3): …refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

[22] Art. 52 (4): …ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers.

[23] Art. 52 (5): …ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

[24] Art. 52 (6): …ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budge.

就該等對於會員國設立獨立專責監管機關之要求，身為歐盟會員國之英國當然必須遵從。事實上英國資料保護法第一個版本早在 1984 年出現並成立相對應之監管與個資保護機構「資料保護登記官(Data Protection Register)」，其後為了因應歐盟資料保護指令(Directive 95/46/EC)，英國有了第二版本之資料保護法(Data Protection 1998) [25]，並將前述之保護官變更為現今的資訊委員(Information Commissioner)而作為資料保護之監管機關，並陸續地將包括了政府資訊公開法(Freedom of Information Act 2000)、隱私與電子通訊規則(Privacy and Electronic Communications Regulations 2003)以及環境資訊規則(Environmental Information Regulations 2004)等所有與資訊相關之法規納入整合[26]。

(二) 資訊委員的職權

此部分在英國的具體實踐上，英國 2018 年資料保護法(Data Protection Act 2018, DPA 2018)在其第 1 條之立法意旨當中，於第 1 項揭示該法係供個人資料處理[27]行為所遵循，並隨即於同條第 2 項說明 DPA 2018 所指的大多數個資處理均遵循 GDPR；更於第 2 條第 1 項將 GDPR 明定為個資保護規範來源之一。因此，關於資訊委員之設置、任務及職權在 DPA 2018 第五部分第 114 條規範資訊委員之機關於新法中依然持續，第 115 條則說明其職權，此處亦明白揭示資訊委員之一般職權與保障機關功能等係依循 GDPR。另除了 GDPR 本身所規範的各國個資保護機關功能以外，其他英國所特有之一般性保障功能規範則在第 116 條以及附件 13 當中。綜合 GDPR 以及 DPA 2018 所規範之

[25] 關於 1998 年英國資料保護法，尤其是關於當事人權利之介紹，參：李振瑋、江耀國，英國資料保護法中資料所有人權利之研究 – 兼論我國個資法之相關規範及案例，中原財經法學，第 24 期，2010 年 6 月，頁 29-86。

[26] 在此時期關於英國個資保護辦公室更為詳細的介紹，請參：翁逸泓、廖福特，私生活權利：探索歐洲，反思台灣，台北：新學林出版，2014 年 12 月，頁 249-280。

[27] 由於 GDPR 第 4 條第 2 款在定義上，即將「處理(processing)」之內涵擴張至包含了我國個資法上「蒐集」、「處理」與「利用」之所有階段，因此英國 DPA 2018 亦依循 GDPR 之定義而規範。

英國資訊委員增加之保障功能來看，現任英國資訊委員 Elizabeth Denham 依循 Raab 與 Bennett 見解[28]，將其分類為：監察使、審核(audit)、諮詢者、教育者、政策建議者、協調者、執行者以及國際（個資保護）大使等不同的「工具」角色[29]。

所謂「監察使(ombudsman)」即以監察之方式確認資料控管者或受託處理者是否遵循 GDPR 與 DPA 2018，而據統計大多數之個資侵害爭議案源均來自錄影監視器與個資爭議以及從搜尋引擎移除個資等被遺忘權(the right to be forgotten)之行使[30]；審核係指資訊委員依法查閱資料控管者處理資料之數位足跡，以確保其遵循個資規範而使個資保護框架具良好實踐，態樣包含風險檢視與審核後所提供之建議等；至於近年作為諮詢者角色最特殊之職權行使，或許是其開始建立管制沙盒(sandbox)使得科技發展之應用有機會以試驗性之方式與公、私領域之相關法規範銜接。至於以執行者來說，基於其除了可以對資料控管者與受託處理者處以罰鍰外，更具可停止個資傳輸之強制處分權，在個案選擇適用不同的執行工具，考量之點則為對於侵害型態本質與嚴重程度之風險評估、個資之敏感性、受侵害之當事人人數、公眾關切程度、公共利益以及其他執行機關是否已然開始執行相關處分等，更重要者，資訊委員通常亦將侵害個資之單位或個人的態度與行止納入考量[31]。

最後，DPA 2018 對於資訊委員賦予 GDPR 所未規範之國際合作職權，如與其他國家個資保護專責機關之合作、履行國際個資保護規

[28] C.J Bennett and C.D Raab, The Governance of Privacy: Policy Instruments in Global Perspective (Cambridge MA: MIT Press, 2006).

[29] ICO, Money, Law and Courage: the Varied Roles of the UK Information Commissioner, 15 March 2018. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/03/money-law-and-courage-the-varied-roles-of-the-uk-information-commissioner/.

[30] ICO, Annual report 2017-18, 19 July 2018. Available at: https://ico.org.uk/media/about-the-ico/documents/2259463/annual-report-201718.pdf.

[31] ICO, 2016. 'Overview of the General Data Protection Regulation (GDPR)'. Available at: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/.

範框架之義務，以及與歐盟會員國互助合作執行個資保護規範之履行等，其中在附件 13 的第 1 條第 i 款特別提出，資訊委員須與 EDPB 尤其是關於法律執行指令(Law Enforcement Directive)之層次上，相互合作。最為特殊者在於附件 13 第 2 條明文授與資訊委員因為執行相關通知職權而有相對應之有限度調查權、矯正權與指導權等，得命資料控管者或受託處理者為一定之作為，使 ICO 不致成為無執行力的機關。所謂的「通知」，包括有第 149 條的因資訊委員認為資料控管者已然或正在違反資料保護法規定之各項原則時，應考量該違反行為是否已對或將對任何人造成損害，而要求其於期限內採取特定之行為，或於期限屆滿後禁止進行特定之行為，甚至是在期限屆滿後禁止處理個資之執行通知(Enforcement Notice)；第 142 條的資訊通知(information notice)，使得資訊委員得要求資料控管者或受託處理者提供資訊使其執行資訊委員之職權；以及第 155 條關於處罰之通知等。

在 DPA 2018 本文中亦要求資訊委員就數個不同領域特殊個資處理面向，有提供行為準則(codes of practice)之義務，包括了第 121 條關於資料分享問題，資訊委員在行為準則中必須考量當事人與他人對於個資規範之適足性。第 122 條關於行銷之行為準則中較特殊者，係其除必須考量 GDPR 外，在行銷面向關於使用網路與電子通訊作為媒介平台者，也應當將英國本身於 2018 年修正的 2003 年隱私與電子通訊（歐盟指令）規則(Privacy and Electronic Communications (EC Directive) Regulations)納入考量。另外，DPA 2018 第 123 條則對應 GDPR 此次修法重點之一關於兒童個資權利之特別保護，對於資訊社會之服務而有關於個資近用之情狀，資訊委員有義務提出適當的分齡準則。第 124 條則就資訊社會中與個資保護權利經常發生競合之新聞自由以及表現自由面向，要求資訊委員對於記者近用個資事項提出相關準則。

最後，因為英國之專責個資保護監管機關係具有集權性質之機關，因此地方政府並無對應專責機關之設置，而依據 DPA 2018 在第 69 條

以下規範，中央與地方之公務機關均須有 DPO 之設立。DPO 與中央專責監管機關之間之關係，大多為該機關組織關於個資事件之通報窗口，以及教育宣導之用，尚無類似我國地方政府消費者保護官制度之獨立職權，而較傾向作為聯繫單位之用，而中央專責機關得對其在一定程度上指揮監督。[32]

二、 個人資料特定目的外利用之要件

就一般個資特定目的外利用而言，英國 DPA 2018 並無特殊規範，原則上均參照 GDPR 之規範：在 DAP 2018 第 87 條，規範即與 GDPR 如出一徹。

事實上 ICO 認為 GDPR 並沒有完全禁止目的外利用，而僅是需合於一定之限制條件。[33]從本質上講，如果個資處理的目的隨時間而改變，或者控管者想將資料用於其原本未曾想到的新目的，則控管者只能在以下情況下進行：

1. 新目的與原始目的兼容；
2. 新的目的獲得當事人的特定同意；
3. 依據明確的法律規定，而該規定要求或允許出於公共利益的目的進行新的處理，例如公共機構的新功能等。

而如果資料控管者對原蒐集個資的目的與新目的是兼容(compatible)的，則無需新的合法依據即可進行進一步處理。但是，如果資料控管者最初是以同意作為蒐集個資的基礎，則通常需要再次獲得同意，以確保資料控管者的新處理合於公正、合法原則。

就 GDPR 與 DPA 2018 言，所謂「兼容」例如出於公共利益的檔案

[32] 關於 DPO 之設置、職權與內涵等，請參考本報告後續章節。
[33] ICO, Principle (b): Purpose limitation, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/.

保存目的、科學或歷史研究目的和統計目的之處理，不應視為不符合原始目的，且兼容應考量資料控管者的原始目的與新目的之間的任何關係、資料控管者最初蒐集當事人資料的環境，尤其是資料控管者與當事人的關係以及他們合理期望的結果、個人資料的性質，例如其是否特別敏感、新的處理行為可能對當事人產生之後果，和是否有適當的保護措施，例如加密或假名化等作為。

通常，如果新目的與原始目的非常不同，令人意外或對個人造成不合理之影響，則可能與資料控管者的原始目的不符。事實上，資料控管者通常可能需要徵得特定同意才能使用或揭露用於此類目的之資料。

綜言之，此部分英國並無異於 GDPR 之特殊規範。

GDPR 對於特種個資之處理言，其基本立場乃原則上不得處理，例外僅於符合法定要件時得予處理，並於 GDPR 第 9 條第 2 項明定例外之情形。須注意者，雖然 GDPR 在歐盟法架構上為規則之層級，因此理論上需直接一體適用在各會員國內，但 GDPR 為調和各會員國個資保護落差以及與其他基本權利與自由保障事項之競合問題，因此其中不乏給予各會員國在一定要件下，透過立法創設較 GDPR 更大的發揮空間的判斷餘地，例如其第 9 條第 g、h、i、j 款分別就：

1. 與其所欲達成目的間具合理關聯之比例性(proportionate)，維護個人資料保護權利之本質，並定有保護當事人基本權利及利益之適當特殊措施，而基於有重大之公益理由，認有必要者；
2. 出於健康照護或為判斷受僱者工作能力之勞動醫學，為了醫學上之診斷、健康或社會領域之照護或治療或為了健康或社會領域之體系或服務之管理，依據歐盟法、會員國之法令或與擔任健康相關職業之成員間簽訂之契約，並符合第 3 項所定要件及保障，而認有必要者；

3. 係於公共衛生領域基於公益理由，例如為防範跨境之嚴重健康危害或為維護健康照護及醫藥產品的高品質及安全標準，並已依歐盟法或會員國法令採行維護當事人權利及自由之適當特殊措施，而認有必要者；以及
4. 依據歐盟法或會員國法令，與其所欲達成目的間具合理關聯性，維護個人資料保護權利之本質，並訂有保護當事人基本權利及利益之適當特殊措施，而依據第 89 條第 1 項基於公益之檔案儲存目的、學術或歷史研究目的以及統計目的，認有必要者等。

對於 GDPR 之特種個資規範，英國 DPA 2018 原則上係依照 GDPR 對於特種個資禁止處理，例外允許處理之情狀，除 GDPR 第 9 條第 2 項各款外，依照前述對會員國之授權，於 DPA 2018 第 10 條第 1 款[34]，特別針對實質公共利益之具體內涵，規範在 DPA 2018 附件 1 第 2 部分，而將關於健康與社會照護、公共衛生、以及檔案儲存、研究與統計等類型，規範在 DPA 2018 附件 1 第 1 部分。

- 利益衡量

詳言之，英國 DPA 2018 之立法規範模式在相當程度上適度地放寬了特種個資之應用。以下對 DPA 2018 附件 1，亦即特種資料例外得處理之情狀加以說明：

1. 健康與社會照護目的

   於為健康與社會照護目的下而具有必要性時，方得處理特種個資。此處之「健康與社會照護目的」，意指預防醫學或職業醫

[34] 另外，尚有非特種個資的 GDPR 第 9 條第 2 項第 b 款之關於勞動就業、社會安全與社會照顧之例外豁免事項。

學[35]、對勞工工作能力之評估、醫學診斷、健康照護或治療之提供、社會照護之提供、或基於健康或社會照護系統或服務之所需。另外，基於此項例外而得對特種個資處理時亦需考量 GDPR 第 9 條第 3 項及 DPA 2018 第 11 條，需資料受託處理者為負擔健康或社會照護專業責任者，或其他在該等情境下對於履行法定義務而負擔保密義務者。

2. 公共衛生目的

於為公共衛生目的下而具有必要性時，且資料受託處理者為負擔健康或社會照護專業責任者，或其他在該等情境下對於履行法定義務而負擔保密義務者，方得處理特種個資。

3. 為檔案儲存、學術或歷史研究與統計目的

於為檔案儲存、學術或歷史研究與統計等目的而具有必要性時，且具有 GDPR 第 89 條第 1 項及 DPA 2018 第 19 條相對應之保護措施，並存在有公共利益。此時，該等保護措施應確認已同時備妥技術上及組織上之措施[36]，特別是用以確保資料最小蒐集原則之落實。此時只要上開目的能真實地實現，則該等措施得包括假名化。再者，如需進一步處理個資時，於該等處理不允許或不再允許再識別當事人時，即符合所謂實現前開目的之要件。

4. 公共利益

關於究竟何謂「公共利益」，向來在我國關於個資法相關解釋上發生爭議；英國 DPA 2018 則在附件 1 第 2 部分有相對詳細

[35] 所謂職業醫學乃是關於工作場所的健康維護，包括疾病和傷害的預防和治療而與醫學相關者，除前述主要目的外，其次要目標包括維持和提高工作場所的生產力和社會適應能力等。在台灣亦有稱之勞動安全醫學等。

[36] 本報告對此部分於第三部分關於去識別化問題之討論將詳細說明。

之說明。在該部分之公共利益作為特種個資例外得處理時，所有以下例外情狀均須存有適當政策文件(appropriate policy document)。在此，該等政策文件依照附件 1 第 4 部分之補充，係指資料控管者必須在特種個資例外地允許被處理時即有該等個資保護政策[37]。

至於該等（個資保護）政策之內容必須包含：(a) 解釋資料控管者對於 GDPR 第 5 條所包含之處理個人資料各項基本原則就現為處理個資之對應行為；以及(b)解釋資料控管者留存與確保處理之個資係符合個資保護之程序的個資政策，其中並須包含個資留存時間。須注意者，本報告對此認為該等時間長短之個資保護政策說明，依照前項關於比例原則之必要性要求，當然不可以一律規範永久留存，或是比例不當之長久時間[38]。再者，依據附件 1 第 40 段該個資保護政策之存在，起期應為資料控管者開始處理[39]個資時；終期則為資料控管者停止處理個資後六個月。

又，同樣地依據附件 1 第 40 段，個資留存於資料控管者之相關期間內，資料控管者均應有個資保護政策，並應注意持續審查(review)其是否能跟上該時代之科技進展而與時俱進，以及無償提供資訊委員相關政策。

最後，依據 GDPR 第 30 條，資料控管者或其代理人應維護其處理個資之活動紀錄，在此 DPA 2018 規範處理特種個資時亦同。此時其必須包含得例外地處理特種個資之條件為何，而在說明該等例外情狀時，也要詳細地說明為何其能通過 GDPR 第 5 條合法處理個資原則之要求，並載明為何該等個資能留存，

[37] Paragraph 38, Part 4, Schedule 1, DPA 2018.
[38] Paragraph 39, Part 4, Schedule 1, DPA 2018.
[39] 須注意者，GDPR 與 DPA 2018 之處理係包含個資之蒐集等態樣。

並在留存原因不復存在時，刪除該特種個資[40]。在說明以公共利益作為得處理特種個資之共同要件後，DPA 2018 則分別明定各種所謂「公共利益」之態樣：

(1) 法規與政府要求:為履行法律義務或政府運作功能所必要，且具實質之公共利益並有必要性[41]；
(2) 司法與立法行政所需，且有必要性[42]；
(3) 平等對待或平等機會：如果是為了在群體中辨識或者審查該群體間個別權利主體是否在機會或待遇上，就強化實現平等原則而有必要處理特種個資者，即應認為有公共利益存在。

此處所謂「群體間」所指為何？因為要處理的是特種個資的問題，所以指的是不同種族間之人、不同宗教或哲學信仰群體間之人、不同生理或心理健康狀態群體間之人、不同性取向群體間之人等。

須注意者,此處關於平等對待或平等機會相關之公共利益，解釋上不包括對特定當事人就平等對待或平等機會而給予之目的，也就是不包括在該等群體內特定之個人。例如，就身障者給予特殊照顧的情狀下，需審核該身障者群體間當事人之特種個資（健康資料)，以確認是否符合所謂身障者之條件而予以對待，此係公共利益；但不得僅針對某特定人審查其健康資料辨識該特定人是否為身障者。再者，該等因審查而處理特種個資之行為不得造成實質損害或個人之心神上痛苦[43]。

[40] Paragraph 41, Part 4, Schedule 1, DPA 2018.
[41] Paragraph 6, Part 2, Schedule 1, DPA 2018.
[42] Paragraph 7, Part 2, Schedule 1, DPA 2018.
[43] Paragraph 8, Part 2, Schedule 1, DPA 2018.

(4) 於組織資深層級之種族與族群多元化：此公共利益之要件需為相關個資攸關種族與族群起源，而於個資處理中辨識適合之個人為特定組織之資深職位，此時為促進或維持在組織或組織中擔任高級職務的個人的種族和民族血統的多樣性而必須，並於此條件下毋需經由當事人同意而可合理進行[44]。簡言之，乃是為了促使組織中高層之資深階層人士能盡量地在族群與種族上具多元化，而得處理該等特種個資。在此情況下，需注意資料控管者要能有合理確信當事人若知此情事即會同意個資處理，且不知當事人對其同意加以保留[45]（此等保留不包括當事人單純對同意之意思表示未回覆）[46]；亦需注意前述之因促進多元化而處理個資之行為不得造成當事人實質危害或實質損害[47]。在此，所謂「資深職位(senior position)」係指法人團體之董事、幹事（負責組織整體管理之事）、或其他類似職級之人，或有限責任合夥企業的成員、根據 1890 年《合夥企業法》中的合夥人，或根據 1907 年《有限合夥法》登記的合夥企業，或根據英國境外國家或地區法律形成的類似性質的實體[48]。而在組織之中，非該等職位但係為資深經理人者，亦同。[49]在此，所謂「資深經理人(Senior manager)」係指決定如何管理或組織整個或大部分組織的活動，或實際管理或組織全部或部分該等活動之人[50]。

(5) （事後）阻止或（事前）防止非法行為：此特種個資允為處理之要件為具防止或避免非法之行為，並須在未經當事人同意之情形下為之，以免損害該公共利益之目的；該等

[44] Paragraph 9(1), Part 2, Schedule 1, DPA 2018.
[45] Paragraph 9(2), Part 2, Schedule 1, DPA 2018.
[46] Paragraph 9(7), Part 2, Schedule 1, DPA 2018.
[47] Paragraph 9(3), Part 2, Schedule 1, DPA 2018.
[48] Paragraph 9(5), Part 2, Schedule 1, DPA 2018.
[49] Paragraph 9(4), Part 2, Schedule 1, DPA 2018.
[50] Paragraph 9(6), Part 2, Schedule 1, DPA 2018.

處理並須為實質公共利益所必須[51]。如果該等處理個資之行為包括向主管機關揭露個人資料，或為預備揭露個人資料而進行，則即便在進行處理時，資料控管者並無適當個資保護政策，仍滿足例外得處理個資之條件[52]。在此，違法行為包括未遂[53]。

(6) 保障公眾避免不誠實：須在未經當事人同意之情形下為之，以免損害該公共利益之目的；該等處理並須為實質公共利益所必須。此處之「不誠實（dishonest）」係指不實、瀆職或其他嚴重不當行為、（資格條件）不適合或（能力）不稱職、機構或協會管理不善（未盡善良管理人義務），或機構或協會提供的服務未成[54]。

(7) 關於違法或不實行為之管制條件[55]；

(8) 關於違法或不實行為之報導[56]；

(9) 防止詐欺[57]；

(10) 涉嫌資助恐怖主義或洗錢[58]；

(11) 為有特定身心障礙或醫療狀況的個人提供支援：非營利組織提供對身心障礙或醫療支持之組織，於提供揭露種族或族群血統的個人資料、遺傳資料或生物特徵資料、有關健康之資料或個人有關性生活或性取向的個人資料時，符合提高大眾對身心障礙或醫療狀況的認識或向屬於前述狀況之個人提供支助，或使此類個人能夠相互提供支助，而未經當事人同意，可合理進行，以及出於重大公共利益的原

[51] Paragraph 10(1), Part 2, Schedule 1, DPA 2018.
[52] Paragraph 10(2), Part 2, Schedule 1, DPA 2018.
[53] Paragraph 10(3), Part 2, Schedule 1, DPA 2018.
[54] Paragraph 11, Part 2, Schedule 1, DPA 2018.
[55] Paragraph 12, Part 2, Schedule 1, DPA 2018.
[56] Paragraph 13, Part 2, Schedule 1, DPA 2018.
[57] Paragraph 14, Part 2, Schedule 1, DPA 2018. 對應之法規為 section 68 of the Serious Crime Act 2007。
[58] Paragraph 15, Part 2, Schedule 1, DPA 2018. 對應之法規為 section 21CA of the Terrorism Act 2000 及 section 339ZB of the Proceeds of Crime Act 2002。

因具必要性[59]。此時資料控管者應有合理確信當事人若知此情事即會同意個資處理，且不知當事人對其同意加以保留（此等保留不包括當事人單純對同意之意思表示未回覆）[60]。

(12) 輔導等；

(13) 保護兒童和處境危險的個人：此處之危險處境意指避免滿18歲之人在需照護或支持之情況下而受忽視或身體與精神上傷害，而所指之兒童為未滿18歲之自然人[61]；

(14) 保障特定人士之經濟福祉：為保障年滿18歲以上而陷於經濟危機人士之經濟福祉目的之所需，該等個資與健康相關，且在某情況下當事人不能同意、或不能合理地期望資料控管者獲得當事人的同意、或如獲當事人同意將妨害個資處理之目的等原因而未得當事人同意[62]，另外，所謂經濟危機，指因身體或精神傷害、疾病或身心障礙而未能保護個人經濟福祉之情形[63]；

(15) 保險：為保險目的揭露特種資料而有必須，可在未獲當事人同意下合理實現，此時需資料控管者無法被期待能合理地獲得當事人同意，或資料控管者不知當事人保留同意（此等保留不包括當事人單純對同意之意思表示未回覆）。然處理的目的不是就當事人採取措施或決定，以及當事人本身並沒有，也不應獲得根據保險目的涉及的保險契約對被保險人的權利或與該人有關的權利或義務，或與此類契約有關的其他權利或義務[64]。在此，「保險契約」是指一般保險或長期保險契約，而「保險目的」是指就保險契約提供意見、安排、承保或管理；根據保險契約管理索賠，或行使

[59] Paragraph 16(1)-(3), Part 2, Schedule 1, DPA 2018. 對應之法規為 Equality Act 2010。
[60] Paragraph 16(4)-(6), Part 2, Schedule 1, DPA 2018.
[61] Paragraph 18, Part 2, Schedule 1, DPA 2018.
[62] Paragraph 19(1)-(2), Part 2, Schedule 1, DPA 2018.
[63] Paragraph 19(3), Part 2, Schedule 1, DPA 2018.
[64] Paragraph 20(1)-(4), Part 2, Schedule 1, DPA 2018.

與保險契約有關的權利或義務，包括依法產生的權利或義務[65]。

(16) 退休金[66]；

(17) 政黨：關於顯露個人政治意見之個資，或登記於政黨、選舉與公投法(Political Parties, Elections and Referendums Act 2000)之個資而與個人或組織之政治活動目的有必要者，或未滿足上述條件，但可能造成對個人之實質損害或造成實質憂擾(substantial distress)、當事人（或當事人之一）已書面聲明通知資料控管者，要求資料控管者不得處理該當事人的個人資料（且未書面發出通知撤回該要求）、通知給予資料控管者一個合理的期限，以停止處理此類資料，以及該期限已結束等[67]。在此，「政治活動(political activities)」包含競選、募款、政治調查和個案工作[68]。

(18) （民意代表）當選人請求之回覆[69]：以此目的而處理特種個資，當選人或其授與代理權之人處理特種個資（以當選人之名義為特種個資處理），並與當選人履行職責有關而回應個人（民眾）而具合理性及必要性[70]。依據本項第二段之反面解釋，此時應解釋為其所處理之特種個資為請求該當選人處理之當事人自身之個資。另方面依據第二段，於請求當選人處理非其自身之特種個資時，除須符合前述要件外，並需未獲當事人同意且當事人不能同意處理、不能合理地期待該當選人獲得處理的當事人的同意、獲得當事人的同意將損害當選人採取的行動、或為了第三人的利益言，處理該特種個資是必要時，當事人卻無理地拒絕同意。在此

[65] 對應之規範為 section 22 of the Financial Services and Markets Act 2000。

[66] Paragraph 21, Part 2, Schedule 1, DPA 2018. 對應之法規為 Pension Schemes Act 1993。

[67] Paragraph 22(1)-(3), Part 2, Schedule 1, DPA 2018.

[68] Paragraph 22(4), Part 2, Schedule 1, DPA 2018.

[69] 此即俗稱選民服務條款。

[70] Paragraph 23(1), Part 2, Schedule 1, DPA 2018.

所謂「（民意代表）當選人(elected representative)」[71]係指英國之中央與地方各級民意代表、鄉鎮市長與倫敦（直轄）市長以及警察與具犯罪調查權者[72]；

(19) 當選人之揭露：本項係指對於當選人自身特種個資之揭露，相關要件與限制約略與前項同[73]；

(20) 對當選人關於受刑人之通知[74]；

(21) 司法判決之公開：為法院之判決或裁定或完成該目的具必要性時[75]；

(22) 運動賽事禁藥：此公共利益之目的在消除興奮劑的措施，該等特種個資之處理係由負責消除體育運動、體育賽事或一般體育運動中的興奮劑之機構或協會為之或負責，或向此類機構或協會提供有關興奮劑或疑似使用興奮劑之資訊[76]。

(23) 運動賽事行為標準：為此公共利益旨在保護體育或體育賽事完整性(integrity)的措施而具必要性，此時必須在未徵得當事人同意的情況下進行，以免損害這些目的，或有其他出於重大公共利益的原因且有必要[77]。

三、 去識別化之要件、程序、認定方式等規定

關於去識別化之要件程序與認定等，由於 GDPR 之法位階層級已由指令提升至規則，故就各會員國於法律規範與解釋言，除 GDPR 明文保留給各國另行規定之裁量餘地空間之外，其他部分必須遵循 GDPR 之規定。所以，就去識別化之法律定義，各國認定大致相同，然還是有去識別化後之相對性與絕對性的議題尚待解決。

[71] Paragraph 23(3), Part 2, Schedule 1, DPA 2018.
[72] Paragraph 23(3)(m), Part 2, Schedule 1, DPA 2018.
[73] Paragraph 24, Part 2, Schedule 1, DPA 2018.
[74] Paragraph 25, Part 2, Schedule 1, DPA 2018.
[75] Paragraph 26, Part 2, Schedule 1, DPA 2018.
[76] Paragraph 27, Part 2, Schedule 1, DPA 2018.
[77] Paragraph 28, Part 2, Schedule 1, DPA 2018.

(一) GDPR 層級

按 GDPR 第 4 條第 5 款,「假名化」Pseudonymisierung 是指該處理個人資料的方式使個人資料在沒有額外的其他資訊情況下，無法歸屬特定的當事人，而該等所謂「額外的資訊」必須符合包括下列要件：(1) 分開存放；(2) 需要採取技術性和組織性措施等保護措施以確保個人資料，不會被使用識別或得識別特定自然人。若透過其他額外的附加資訊，得以確認特定自然人時，則該筆資訊應被視為可識別的個人資料。

為此，如欲判斷一個自然人是否可識別，則其判斷標準應考慮資料控管者或任何其他人通常自行決定可能使用的所有手段，以直接或間接識別自然人，例如挑選[78]、排除等。實務判定上必須釐清的是當資料控管者沒有在事件層面（event-level）中刪除原來（可識別）的資料時，即變相將資料集(data set)的部分資料，例如已經刪除或被掩蓋的可識別身分資料轉交其他方,則所轉交的資料實際上仍然屬於個人資料。換言之，只有當資料控管者將資料聚合（aggregate）到某個程度以後，已經無法再識別資料中的個別事件（individual events）時，資料集才符合匿名化的標準。再者，所謂「任何其他人」在解釋上包括各潛在個資再利用（處理）者或其他對獲取資料有動機而感到興趣的權利主體，尤其是公務機關。

復次，所謂「技術性和組織性措施等保護措施」無論是依照歐盟之資料保護指令、GDPR、歐盟第 29 條個資保護工作小組或是英國 ICO 之認定，均須回歸到原始的資料保護指令之定義。因此已假名化之個人資料，且可透過使用額外資訊而識別出當事人身分者，仍應被認為屬於可得識別之當事人的資訊。

[78] 有效將資料匿名化能防止他人透過資料集的兩項記錄而產生關聯,或從兩個獨立的資料集中產生關聯，繼而從資料集中挑出（singling out）某特定人士，避免從資料集中推論出某人的資料的可能性。一般而言，直接清除可識別身分的元素並不能絕對防止當事人被識別。

就前者的「技術保護措施」方面言，為決定當事人是否可被識別，應考慮到所有可能合理使用之方法，例如由控管者自己或透過他人指認以直接或間接地識別該當事人。為確認何為可合理使用作為識別當事人之方法，應考慮所有客觀因素，諸如：識別所需之成本與時間，並考慮到資料處理當時現有之技術及科技發展。在確定是否可用於識別自然人的方式時，應考慮到資料處理時的科技和發展情況，使用所有客觀因素，如識別成本和所需時間[79]。準此，經由匿名化（anonym）的資料或以匿名方式以致當事人無法被識別或不再被識別，亦即無法被識別或不可能被識別的個人資料，包括由統計或研究目的產出的資料等，原則上並不在個人資料保護之列。而匿名化與假名化二者之區別標準在於判定何種結果才屬於可接受的資料再識別風險。換言之，第三方在決定如何使用資料，尤其當涉及基於其自身目的而組合有關資料時，便必須考慮前述與背景和情況有關的因素，包括原資料控管者採用的假名化技術之具體特點等，這是因為再次處理資料將導致第三方擔負不同保護責任，如果這些元素和特點將對當事人產生不能接受的身分識別風險，此時，當事人便應當再次受個資保護法律所規範[80]。

進一步言，在很多情狀下該等資料僅僅適用於第三方再利用篩選過的資料有限披露或公開，而不適用於大量的資訊公開（如政府資訊公開）以及許可條件下的政府資訊再利用（Public Sector Information, PSI）。關於此，本報告作者之一曾於其他論述歸納目前國際上對於政府所擁有資訊之接近及利用，可以化約為三個不同之模式，該三模式並可以其進程歸納為三個階段：政府資訊公開(Freedom of Information, FOIA)階段、政府資訊再利用(Re-use of PSI)階段、以及開放政府資料

[79] GDPR 前言第 26 點參照。

[80] 換句話說，在我國開放政府資料個案如 MyData 或是健保署健康存證中當事人健保資料以 SDK 方式介接進入其他企業或個人時，均應加以考量。

(Open Government Data)階段。[81]

在後二階段[82]，政府對於資料之再利用有以下三種選擇:(1)不公開個人資料作再利用；(2)將個人資料轉換成匿名形式(通常會轉換成聚合性的統計資料)，且僅公開已經匿名化處理的資料作再利用；(3)公開個人資料作再利用。此時公務部門必須相對應有所作為，以便達成 PSI 再利用之目的。

關於新興科技發展的隱私與個人資料保護風險問題，因為科技於深度應用化後較難加以控制與改變之關係，如果能在科技研發的早期即導入風險避免與風險識別之概念，則較為有效。不過科技於早期設計研發階段其未來影響較難以預估，因此造成早期介入風險防止之困難度與真正確切實效問題[83]。因此在確定何時以及如何發布匿名資料時，基於公開資料的原因將影響資料控管者進行揭露的方式，會因為身分識別的風險和後果會有所不同，一旦依據開放政府資料之許可而公開了資料，就可能無法保護其免於進一步利用或揭露或確保其安全。因此在資訊公開或政府開放資料時會因為範圍更廣而造成風險更大。[84]

須注意者，儘管匿名資料屬於許可開放的範圍，而開放政府資料之許可即便是明確規定不允許使用者和再使用者以能夠進行重新識別的方式使用資料，但是，實際上這可能難以執行或甚至無法執行。[85]

又，既然匿名及聚合的資料庫不應該允許對某個人再識別，因此在解釋上不應包含有任何的個人資料。為使得開放之資料有其真正之

---

[81] 翁逸泓，2019 年 2 月，開放全民電子健康資料加值應用之個資保護問題－以英國經驗為例，月旦法學雜誌，第 285 期，頁 147-149。

[82] 事實上第三個階段僅是第二個階段之進階類型，重點著重在開放給「任何人」使用，並在程序上使其資料之利用更有效率。

[83] 此即所謂「Collingridge dilemma」，多應用於科技發展之社會控制問題。David Collingridge (1980). *The Social Control of Technology*. New York: St. Martin's Press.

[84] ICO, Anonymisation: managing data protection risk code of practice, https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf, 17.

[85] Ibid, 38.

實用性，資料匿名化個人資料的處理需以不可逆轉的方式防止身分識別。進行相關操作時，資料控管者應先考慮一切用於識別身分的「合理可行」（likely reasonably）方法（不論是資料控管者還是任何第三方均為如此），才考慮其他的相關因素或要件。

- 匿名化與假名化之實際操作程序

對於資料的聚合和匿名一般都在較早期由資料控管者或者可靠的第三方代表在有必備的專業技能之情況下，以一個或者多個資料控管者的名義進行。換言之，該等處理不可由再利用者為之；另外，為了避免利益衝突，操作上必須要能夠確保第三方機構實行的聚合和假名化操作不存在任何潛在利益衝突及個人資料僅用來進行假名，並採取有必要的保障措施達到這樣的效果。不僅如此，第三方還應保證通過聚合和假名資料獲取的資料集在使用過後，應立即刪除原資料集。綜言之，假名化後，意欲回溯得到連結（re-link）而應用的個人資料，需頗耗費時間精力等成本，或部分去識別化方法甚至難以回復而辨識個人（此即非經由「合理（reasonable）」手段），而逸脫於可得識別（identifiable）個人的個人資料定義範疇之外，並以之作為個人資料保護之手段。

須注意者，傳統上認為難以回溯連結的「永久去連結」，經過資料探勘（data mining）與巨量資料(big data)技術發展後，已經使資料與個人身分永久分離的手段，失去效用，而僅能使資料與個人身分暫時分離。尤有甚者，隨著片段真實性資料本身或是經過巨量資料處理後加值衍生物的長期累積膨脹，破解去識別化的機會大幅提高。傳統去識別化的方法，已經輕易地被許多合理使用下的巨量資料分析結果所崩解。換句話說，去識別化的確可以在相當程度上降低個資風險，但是卻絕不可能使風險萎縮為零，而這種降低個資風險的技術，確有可能

因為巨量資料技術應用，而趨近於無效（雖不一定至完全無效）[86]。

相對地，匿名化之方法相當多，通常以匿名化編碼（coded）或永久去連結（de-linked）等方式為之。前者係暫時將原有個人識別資料部分，以特定文字或數字取代，達到匿名效果；在解碼時，則可回溯個人識別資料。後者則是一開始便放棄對照的解碼方式，回溯連結的可能性相對較小。對此，或許資料控管者應專注於能逆轉（reverse）匿名化技術的實際手段，尤其手段所需要的成本和技術訣竅，以及評估手段的可行性和效能。故此，應當注意識別技術的風險會隨時間推移而增加，並且取決於資訊和通訊技術的發展，而有關的法律規定也應當以技術中立（technologically neutral）的方式進行立法，如能同時對通訊科技的發展潛能加以預設考慮，則符合風險預防之思考。

有效將資料匿名化能防止他人透過資料集的兩項記錄而產生關聯，或從兩個獨立的資料集中產生關聯，繼而從資料集中挑出/ 識別出（singling out）某特定人士，避免從資料集中推論出某人的資料的可能性。一般而言，直接清除可識別身分的元素並不能絕對防止當事人被識別，反之，往往需要採取額外措施，而且也取決於匿名化處理的手段和匿名化所希望達到的目的。

就後者「組織性措施保護措施」言，則首應考慮相關的法規範和處理環境，並建立組織性的專責監管機關，並佐以 DPO 制度之落實。

(二) 英國個人資料保護法制與落實

英國事實上早在 2012 年即由 ICO 發表了 Anonymisation: managing data protection risk code of practice 之報告。該報告之重點大致上主要在於說明匿名化之可行，以及在法律層面上匿名化與英國之 1998 年資料

[86] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' （2014） http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf .

保護法之關係，並提供關於匿名化之優點與建議以及再識別之風險。其中有一個概念相當值得被提出討論，亦即在該行為準則中，ICO 認為只要是對於個資當事人不會造成損害之前提下，資料控管者並非在匿名化個人資料時均須要獲得當事人之同意。

不過，其後基於歐盟第 29 條個資保護工作小組亦發表了第 216 號意見書說明關於匿名技術之問題，因此在相當程度上英國 ICO 此一匿名化行為準則之重要性受到一定程度之衰弱消減。為此，英國 ICO 及其之合作夥伴 The UK Anonymisation Network （UKAN）於 2016 年提出新的「匿名化決策架構 The Anonymisation Decision-Making Framework （ADF）」報告。須注意者，由於該報告出版年係在 GDPR 正式上路之前，因此在文字上仍有關於匿名/假名混淆之情況。例如在 Anonymisation: managing data protection risk code of practice 之報告版本指引中即指出：[87]

…我們使用廣泛的術語「匿名化(anonymisation)」來涵蓋可用於將個人資料轉換為匿名資料的各種技術。例如，我們區分了用於產生集合資訊 (aggregated information) 的匿名化技術以及假名化 (pseudonymisation)，即以個人為單位而產生匿名資料之技術。…

那麼，在 GDPR 修法之後，英國又如何區分匿名與假名？原則上依據 ICO 之區分，仍遵照 GDPR 之規範加以區分。

在匿名方面，ICO 一樣認為這意味著已匿名的個人資料不受 GDPR 約束。因此，匿名化可以成為限制風險以及為當事人帶來益處，也因此 ICO 鼓勵在任何可能的地方對個資進行匿名處理。同時，依照 GDPR 之解釋，ICO 也提醒在嘗試匿名處理資料人數時，應謹慎為之。實際操作上，雖然很多組織或資料控管者通常稱個人資料集為「匿名」時，

[87] ICO, Anonymisation: managing data protection risk code of practice, https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf.

事實上並非如此。為了根據 GDPR 進行真正的匿名處理，ICO 認為必須刪除個人資料中足夠多的元素，這意味著無法再識別該個人。相對地，如果可以隨時使用任何合理可用的方法來重新辨識資料所指向的個人，則該資料將不會被有效匿名，而只會被假名化。這意味著，儘管資料控管者嘗試進行匿名化而逸脫於 GDPR 之範圍，但事實上其仍繼續處理個人資料而為規管範圍。[88]因此無論在定義上、程序要件上，及相關判斷標準上，在未有進一步的更新指引前，均依照 GDPR 之標準與解釋。

不過即便是 GDPR 已然生效且將匿名與假名兩個概念完全區分，至目前為止 ICO 仍未更新關於匿名/假名化之相關指引，仍建議大眾參照舊有之指引與報告。[89]足堪我國借鏡的是，在該報告中對於 2012 年之報告提出總結之觀察一共有二[90]：其一，有效率的匿名（應為假名）化是有可能做到的，不過相對地，無效率之匿名（應為假名）化更容易出現；就法律層面言，要很明確地去釐清在定義上要為「個人資料」劃出一道清楚的界線，有時候是很難做到的。然而很不幸地，對於匿名（應為假名）化之個人資料，一般人通常很容易發生幾個誤解，例如包括了誤解個資之匿名（應為假名）化係關於個人資料之組成成分，但事實上其係資料本身與相關連環境之問題；其二，誤會匿名化以後之個資即為完全無風險之非個人資料，而忽略再識別可能風險；又或認為該等資料便屬於最終之狀態，而不能理解為何對該等資料之利用與再利用仍然需要持續確認個資侵害之可能性[91]。

再者該份報告中，英國資訊委員也在前言很明確地表示，要說出例如「完全匿名化是絕對不可能」、「再識別永遠都有機會」等語是非

[88] ICO, What about anonymised data?, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/, last visited: 2020/6/16.
[89] Ibid.
[90] Mark Elliot, Elaine Mackey Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework, UKAN, 2016, vi.
[91] Mark Elliot, Elaine Mackey Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework, UKAN, 2016, 1.

常容易的，但是要能實際地評估再識別風險以及在資訊近用與個資保護之間求得平衡卻是很難做到的[92]，這尤其是在資料科學與應用技術飛快進步[93]而導致再識別風險提高的今日，更是重大問題之所在。

於該份報告中關於匿名（應為假名）化之相關問題，其核心之主旨在於匿名（應為假名）化的技術本身固然對於資訊安全而言非常地重要，但卻絕對不是最重要的一件事。關於匿名（應為假名）化是否能夠真正地有效率，最重要的焦點反而應該聚焦於需要先認知到匿名（應為假名)化是一個非常由內容決定程序(context-dependent process）之概念，且必須要考慮到該等資料與其相關環境之整體系統，而不僅僅只是技術層面的資訊安全。詳言之，關於匿名（應為假名）化之概念，除了關於資訊安全應有之風險意識與風險管理態度與能力之外，還必須要意識到事實上匿名（應為假名）化的過程本身就是一種決策之行動表彰，該等決策內涵包括例如資料控管者是否應當開放該等資料？如果要開放，又該以何種型態開放[94]？等等問題。因此，技術固然重要，但是如果無法完整地認知整體內容，尤其是必須要考慮的包括資料分享之倫理、透明與公共參與等，更是我國於從事相關實務與研究上所經常忽略者。

- 假名化之類型

倘若就關於假名化之類型加以觀察，該份報告中指出其分類之型

[92] Mark Elliot, Elaine Mackey Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework, UKAN, 2016, vi.

[93] 數位資料的生命週期有六大獨特階段：產生（如社群媒體、電子郵件、上網瀏覽、線上廣告、電子商務、地理定位）、傳送（無線、有線及寬頻網路）、儲存（雲端儲存、「資料湖泊」、快閃記憶體）、處理（企業級及線上雲端伺服器）、使用（網路影片及電信 OTT 影片）及「變現」獲利化（網路廣告、數位行銷管理、進階資料分析）等。甚至，資訊安全也將是數位資料生命週期中維護資料安全性的一大重點，從而相對地再識別化風險將顯著地提升。

[94] Mark Elliot, Elaine Mackey Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework, UKAN, 2016, 2.

態共有四大類型：[95]將直接識別判準標示（direct identifiers）[96]從資料集中移除或以方法隱藏的正式匿名（假名）（Formal Anonymisation）[97]、以不可逆的匿名化方式，例如透過演算法之方式為之的保證匿名（假名）（Guaranteed Anonymisation）[98]、以統計之方式匿名化的統計匿名（假名）（Statistical Anonymisation）[99]等。雖然理論上後兩者似乎是GDPR 所稱之真正的匿名化，但是需要注意的是，事實上即便是此二種方式之匿名化，均仍有再識別之風險存在。

最後一種類型之假名為功能匿名（假名）（Functional Anonymisation）[100]/ 假名，其不僅聚焦於匿名（應為假名）化之與資料相關技術與工具本身，而更擴張至資料環境，並將焦點放在諸如：意圖攻擊匿名資料而將該等資料予以再識別者之動機（此將影響發生之再識別風險事件為何（what），以及為何未發生該等事件（how））；事件所造成之（損害）結果為何；匿名化程序之治理、資訊安全與其他架構之相互影響關係、其他的外部資料與匿名下資料之連結可能性與緊密程度，以及有問題之資料與其他資料之關聯性等。

最後，關於假名化之流程與操作準則，ADF 報告則將其區分為揭露風險評估與控制（Disclosure Risk Assessment and Control）及影響管理（Impact Management），並分別有複雜的子階段。[101]

- 再識別與其防止

[95] 須注意者，於英國當時發布該報告時，GDPR 尚未通過，故尚未清楚定義與區分匿名與假名，因此原文中的匿名，事實上應解為 GDPR 之假名。
[96] 所謂「直接識別判準標示」包括例如特定之識別判準標示、生物特徵替代、轉換式識別判準標示（例如動態 IP）或是功能性識別判準標示（姓名加上住址）等。
[97] Mark Elliot, Elaine Mackey Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework, UKAN, 2016, 17-18.
[98] Mark Elliot, Elaine Mackey Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework, UKAN, 2016, 18-20.
[99] Mark Elliot, Elaine Mackey Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework, UKAN, 2016, 20-21.
[100] Mark Elliot, Elaine Mackey Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework, UKAN, 2016, 21-22.
[101] Ibis, 91-120.

既然無論是何種類型的假名化，均有遭到再識別之可能風險，而除非該等風險係數非常低，否則無法被視為係匿名而應當為 GDPR 所稱之假名，則其決策之原則應注意包括[102]：關於決定資料是否安全，不能夠僅僅單獨考量資料「本身」，但偏廢地忽略資料本身，亦為不足取；假名化係一個製造安全且「有用」資料之過程，但是如果要製造有用之資料，則完全沒有再識別風險是不切實際的；並且，投入個資匿名化之成本與手段必須合於該等資料能被利用價值之比例。最後在假名化環境之架構方面，則應注意資料情狀之監察、風險之分析與控制與影響之管理[103]。

至於對於再識別之防止，係為降低使假名化甚至匿名化失效的最佳手段，對此 DPA 2018 第 171 條與第 172 條之「將去識別化個資重新識別罪」。在第 171 條第 1 項中，明白規範個人因故意或過失對於已去識別化之個資，在未經資料控管者就該等去識別化個資負有法律責任範圍內同意之情況下，將之再識別而得出資訊則係為刑事之犯罪。於第 171 條第 2 項第 a 款，所謂去識別化，指無法將該等資料歸屬於特定之當事人，而所謂的再識別，則在第 171 條 2 項第 b 款中定義為個人以方法造成該等資訊無法再處於前述去識別化之定義狀態下。不過，個人即便為前述之行為，仍有阻卻違法之事由。在第 171 條第 3 項分別規定三款事由，即為防止或偵查犯罪之目的所需而具有必要性；授權機關為執行法律、依法或是依據法院令狀之所需；或是為特定情況下為公共利益而為之。需注意者，此際該再識別之個人負擔舉證責任。第 171 條第 4 項分別規定四款阻卻違法事由，同樣的，以下阻卻違法事由仍須由再識別之個人負擔舉證責任：第 171 條第 4 項第 a 款：為再識別之人之行為係合理信賴其(i) 本身即是該等個資之當事人;(ii)

[102] Mark Elliot, Elaine Mackey Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework, UKAN, 2016, 4-5.
[103] Mark Elliot, Elaine Mackey Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework, UKAN, 2016, 67-117.

經當事人同意[104]；(iii) 如果當事人知道在該等情狀下會被再識別時，一定會予以同意，以及（iv）符合第 172 條之有效性測試構成要件(effectiveness testing conditions)。

第 171 條第 4 項第 b 款：為再識別之人之行為係合理信賴其（i）係為需負擔法律責任之資料控管者；(ii) 經資料控管者同意；(iii) 如果資料控管者知道在該等情狀下會被再識別時，一定會予以同意。

第 171 條第 4 項第 c 款：為再識別之人之行為(i)係為特殊目的；（ii）為新聞、學術、藝術或文學作品之出版；(iii) 合理信賴其再識別係在特定情狀下為了公共利益，且可被正當化。

符合第 172 條之有效性測試構成要件（effectiveness testing conditions)，其係指：該為再識別之人之行為同時符合下列三者：(a) 係在測試該等去識別化個資之效果（例如亂度測試等)；(b) 並非為了意圖造成威脅傷害或侵擾其他個人；(c) 具合理信賴其再識別係在特定情狀下為了公共利益，且可被正當化。該行為人通知資訊委員或是需負擔法律責任之資料控管者，並符合（a）未有遲延；(b) 於可預見情狀下，不晚於 72 小時。此間，如果有一個以上之資料控管者，僅需其中一人或以上被通知即可。

四、 特殊處理情形

在 GDPR 第 9 章中，GDPR 對於個資之特殊處理情形加以規範。在本章所規定之情狀，均為特別需要衡平個人資料保護與其他種類型之基本權利與自由之衝突點，包括：個人資料保護與言論及資訊自由（第 85 條)、官方文件之供公眾接近使用與處理（第 86 條)、國家識別代碼之處理（第 87 條)、僱傭關係資料處理（第 88 條）以及基於公益之檔案儲存目的、基於學術或歷史研究目的以及統計目的之處理(第

[104] 須注意者，英國 DPA 2018 第 172 條第 8 項特別說明，在第 172 條各款的同意中，不包含 GDPR 第 28 條第 10 項，以及 DPA 2018 第 59 條第 8 項、第 105 條第 3 項之同意。

89 條）等個人資料處理之特殊情形，為進一步之規範。在 DPA 2018 中，於其第 6 章第 174 至 176 條規範。以下以英國相關規範為中心，分別討論。

(一) 個人資料保護與言論及資訊自由（GDPR 第 85 條）

1. 對歐盟層級規範與 GDPR 之解析

基於 GDPR 第 85 條第 1 項要求會員國以立法之方式調和個資保護相關的諸項權利以及表現自由以及資訊自由之可能競合，包括了以新聞、學術、藝術與文學為目的之表意與資訊自由類型。在此，必須特別注意的是第 85 條在此不但包含了表現自由，也同時夾帶了資訊權，也就是「知的權利」此等獲取資訊之相關權利。換言之，此時以新聞、學術、藝術與文學為目的之表意行為，以及為此等目的，特別是新聞、學術之目的而得到資訊之權利，均在第 85 條中可與個資保護權利相調和。而在第 2 項中進一步地將前述競合情狀依據比例原則（必要性）之判斷，作為個資保護之例外或是排除(derogation)情狀：而其例外之範圍包括 GDPR 第二章（原則）、第三章（當事人之權利）、第四章（控管者及受託處理者）、第五章（個人資料移轉至第三國或國際組織）、第六章（獨立監管機關）、第七章（合作及一致性）及第九章（特殊資料處理）所定規定。

2. DPA 2018 之規範

需特別注意者，GDPR 在第 85 條第 1 項所謂給予會員國調和空間，也就是「排除(derogation)」，係指會員國可基於本國法律體系或國情而對某些特定之條文規範不予適用。相較於此，英國 DPA 則是在國內法之情況下，對某些規範在適用條文而被違反之情狀下，對行為人給予豁免(exemption)其義務或處罰。

為此，在 DPA 1998 修正至 DPA 2018 時，ICO 即發表對 GDPR 之

對應意見，稱 DPA 1998 相關的第 32、45、與 46 條應維持，並特別考量關於執法之必要性與比例原則[105]。

相較於 GDPR 將第二章至第七章、第九章等範圍包括在調和衡平以新聞、學術、藝術與文學為目的之表意與資訊自由類型，DPA 2018 之範圍則較小，其中在基本原則部分（對應 GDPR 第二章），DPA 2018 對關於 GDPR 第 5 條第 1 項 f 款與第 5 條第 2 項相關原則之例外調和規範，僅包含合法性原則、公平原則、透明原則、最小目的原則、目的原則、正確原則、留存限制原則，而不令資安保障原則與課責原則有所退讓空間。[106]在當事人權利部分，則是 DPA 2018 在對關於 GDPR 第 22 條的相關原則之例外調和規範中，對基於自動化處理決策的類型則無調和規定（沒有例外退讓餘地）。對於 GDPR 第四章的資料控管者與受託處理者之責任，對 DPA 2018 來說則僅在通知責任(GDPR 第 34 條)與在高危險狀態向資訊委員諮詢(GDPR 第 36 條)有調和可能；至於對應 GDPR 其餘章節，則僅有少數國際合作義務可以調和，顯見個資退讓與可能減縮保護之情況較 GDPR 少。[107]

此際，雖然 GDPR 被許多學術上或是實務上的評論者認為是一個限制研究自由或甚至扼殺研究環境與發展想像的規範，但事實上 GDPR 相對資料保護指令而言，已經將包括學術研究表意與獲得資訊之特權予以明文調和，而給予該等特權更寬之空間，甚至符合比例原則之情況下，能突破某些個資保護之基本原則、對當事人之權利保障、對資料控管者責任之排除，以及程序上之救濟效益等。不過，DPA 2018 雖然也賦予此四種類型之表意與資訊權調和空間，卻顯然再度給予一定

[105] ICO, The Information Commissioner's Office (ICO) response to DCMS General Data Protection Regulation (GDPR) derogations call for views, 2017, https://ico.org.uk/media/about-the-ico/consultation-responses/2017/2014036/ico-response-dcms-derogarations-consultation-20170510.pdf.

[106] Paragraph 26(9), Part 5, Schedule 2, DPA 2018.

[107] Miranda Mourby, Heather Gowans, Stergios Aidinlis, Hannah Smith, Jane Kaye, Governance of academic research data under the GDPR—lessons from the UK, International Data Privacy Law, Volume 9, Issue 3, August 2019, 192–206.

程度之限縮[108]。

又，DPA 2018 第 174 條關於執行之層面，將與表現自由此等基本權利與自由保障事項的前述四種特定類型（新聞、學術、藝術與文學）稱作「特殊目的之（個資）事項(special purposes proceedings)」，亦即有關前揭四種類型之個資處理目的，且為第 167 條[109]之司法救濟程序或第 169 條[110]基於其他個資保護規範之損害賠償程序。而資訊委員可對此等競合之衡平做出書面決定，決定之範圍包含在此等特別目的中不允許個資被處理，或是在此前未公開發表的情況下，不許發表關於新聞、學術、藝術或文學之個資的處理。此等書面決定需通知控管者或受託處理者，並載明救濟途徑與確定之期。

需注意者，在 DPA 2018 附件 2 第 5 部分第 26 條第 3 項中載明，如控管者可合理相信該等個資處理不能與特殊目的相提並論，則不適用。另外，該等特殊目的在決定意見是否發表時，其關於公共利益之考量必須慮及表意與資訊自由該等公共利益之重要性。

3. DPA 2018 之實踐

在實踐方面，或許其中較為值得未來國發會或臺灣個資專責機關注意的是在 DPA 2018 附件 2 第 5 部分第 26 條第 6 項，指定實踐準則與指引，分別是 BBC 編輯指引(BBC Editorial Guidelines) [111]、英國通訊管理署廣播指南(Ofcom Broadcasting Code)、編輯實踐準則(Editors' Code of Practice)。

基於對應 DPA 2018，BBC 編輯指引在 2019 年改版，其第 7 章為隱私權，除編輯指引本身外，也考量前述英國通訊管理署廣播指南而

[108] Ibid., 195-196.
[109] 包含（近似）GDPR 第 79 條。
[110] 包含（近似）GDPR 第 82 條。
[111] BBC, The BBC Editorial Standards, http://downloads.bbc.co.uk/guidelines/editorialguidelines/pdfs/bbc-editorial-guidelines-whole-document.pdf, June 2019.

分別就隱私與同意、秘密攝錄、電子記事、秘錄設備、即時串流、私人調查、到戶訪談(Doorstepping)、記者隨同警調行動攝影(Tag-Along Raids)、報導死者訊息、受害與沮喪狀態之人、失蹤人口，以及其他與個人資料相關等涉及表意、資訊自由與個資保護可能競合之特別狀況，給予指引說明，並在指引中特別強調個案中比例原則之權衡、同意程序之特別重要、原則上僅報導公眾人物之私下不正行止或因為其行止而特別受矚目的準公眾人物、特別注意處理個資之目的，以及衡平包括人性尊嚴與公共利益之問題等。

此外，所謂可能被調和之個資保護權利，包括 GDPR 第 2 章的基本原則，包含個資處理原則、合法原則、同意原則、兒童同意原則、特種資料處理原則、犯罪資料處理原則、不需識別處理原則[112]，第 3 章當事人權利保護[113]、第 4 章控管者與受託處理者責任[114]、第 5 章跨境傳輸[115]、以及第 7 章國際合作[116]等。

最後，關於學術研究為目的之表現自由與資訊權之排除/豁免有幾點必須加以特別釐清：

- DPA 2018 第 174 條關於執行之層面雖然規範了四種特定類型，

[112] Chapter II of the GDPR (principles)— (i)Article 5(1)(a) to (e) (principles relating to processing); (ii)Article 6 (lawfulness); (iii)Article 7 (conditions for consent); (iv)Article 8(1) and (2) (child's consent); (v)Article 9 (processing of special categories of data); (vi)Article 10 (data relating to criminal convictions etc); and (vii)Article 11(2) (processing not requiring identification).

[113] Chapter III of the GDPR (rights of the data subject)— (i)Article 13(1) to (3) (personal data collected from data subject: information to be provided); (ii)Article 14(1) to (4) (personal data collected other than from data subject: information to be provided); (iii)Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers); (iv)Article 16 (right to rectification); (v)Article 17(1) and (2) (right to erasure); (vi)Article 18(1)(a), (b) and (d) (restriction of processing); (vii)Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing); (viii)Article 20(1) and (2) (right to data portability); and
(ix)Article 21(1) (objections to processing).

[114] Chapter IV of the GDPR (controller and processor)— (i)Article 34(1) and (4) (communication of personal data breach to the data subject); and (ii)Article 36 (requirement for controller to consult Commissioner prior to high risk processing).

[115] Article 44 (general principles for transfers).

[116] Chapter VII of the GDPR (co-operation and consistency)— (i)Articles 60 to 62 (co-operation), and (ii)Articles 63 to 67 (consistency).

但是在實際落實上，第 174 條第 3 項第 a 款規範有關於在此四種特別類型個資中，資訊委員被賦予能以書面意見決定是否仍可處理個資之權力。而目前在實務上關於第 174 條，資訊委員僅以書面決定放行關於以研究為目的之類型。而所謂以研究為目的，其範圍包含了為使某人發表學術素材(academic material)而進行的任何處理，而該過程尚未由資料控管者出版。

- 在此，資料控管者就學術目的之出版仍須符合關於表現自由與資訊權利之公共利益，於出版其學術文獻時，仍應遵循前述 DPA 2018 附件 2 第 5 部分第 26 條第 6 項相關之實踐準則與指引。
- 實務上除了個資保護在 GDPR 與 DPA 2018 之規範外，另需考量經常發生競合的（資訊）隱私權保障。因此，雖然 GDPR 與 DPA 2018 均適度調和以研究為目的之表意（發表出版）與資訊權利，而使個資保護在經過比例原則檢驗並合於公共利益之情況下成為特權而有所退讓，但是實際上其影響仍有限[117]。
- 關於以研究為目的之類型，最需要注意的是 GDPR 第 85 條並非對學術特權之唯一例外排除規定，GDPR 第 89 條也規範了基於公益之檔案儲存目的、基於學術或歷史研究目的以及統計目的之（概括的）處理特權。就範圍來看，兩者之區別實益在於第 85 條保護的標的是關於任何學術領域之表意與資訊權利，而授權會員國以立法之方式調和其與個資保護之競合；第 89 條則是以科學研究或歷史研究為目的之個資處理，應受適當技術上及組織上保護措施之拘束，該等保護措施得包括假名化，但須於實現以科學研究或歷史研究為目的之範圍，且不允許或無法再識別當事人。關於後者於英國之詳細實踐，見下述。

(二) 官方文件之供公眾接近使用與處理（GDPR 第 86 條）

[117] Miranda Mourby, Heather Gowans, Stergios Aidinlis, Hannah Smith, Jane Kaye, 201.

GDPR 第 86 條規範：公務機關或公務機構或私人機構為履行公共利益而執行職務所持有並存在於官方文件之個人資料，得由該公務機關或機構依其所受拘束之歐盟法或會員國法律規定揭露予同受拘束之公務機關或機構，以調和公眾接近使用官方文件與本規則所定個人資料保護之權利。以英國言，主要規範於政府資訊公開法(FOIA 2000) 以及環境資訊規則(Environmental Information Regulations, EIRs)。

關於 FOIA、EIRs 與個人資料之間之競合衡平問題，資訊委員亦提出個資指引[118]。在指引中說明此等競合問題的第一步驟為判斷在 FOIA 與 EIRs 之程序中是否有涉及在 DPA 2018 規範定義下之個資。

如有，則第二步驟判斷是否為最常涉及之合法、公平與透明原則之個資保護原則[119]，而該等原則之判斷則依照 GDPR 第 6 條之規範標準判斷；又，如為特種個資，則依照 GDPR 第 9 條之規範標準判斷、犯罪資料依照 GDPR 第 10 條之規範標準判斷。如未通過以上之判斷，則不得揭露，且不需考量公共利益之衡量。

第三個階段則衡量是否違背當事人之拒絕權，第四階段為判斷是否係當事人接近利用要求之例外情狀，並考量是否不揭露資料能維護公共利益。最後，第五階段則要求相關機關負擔確認資訊與拒絕資訊公開之義務。

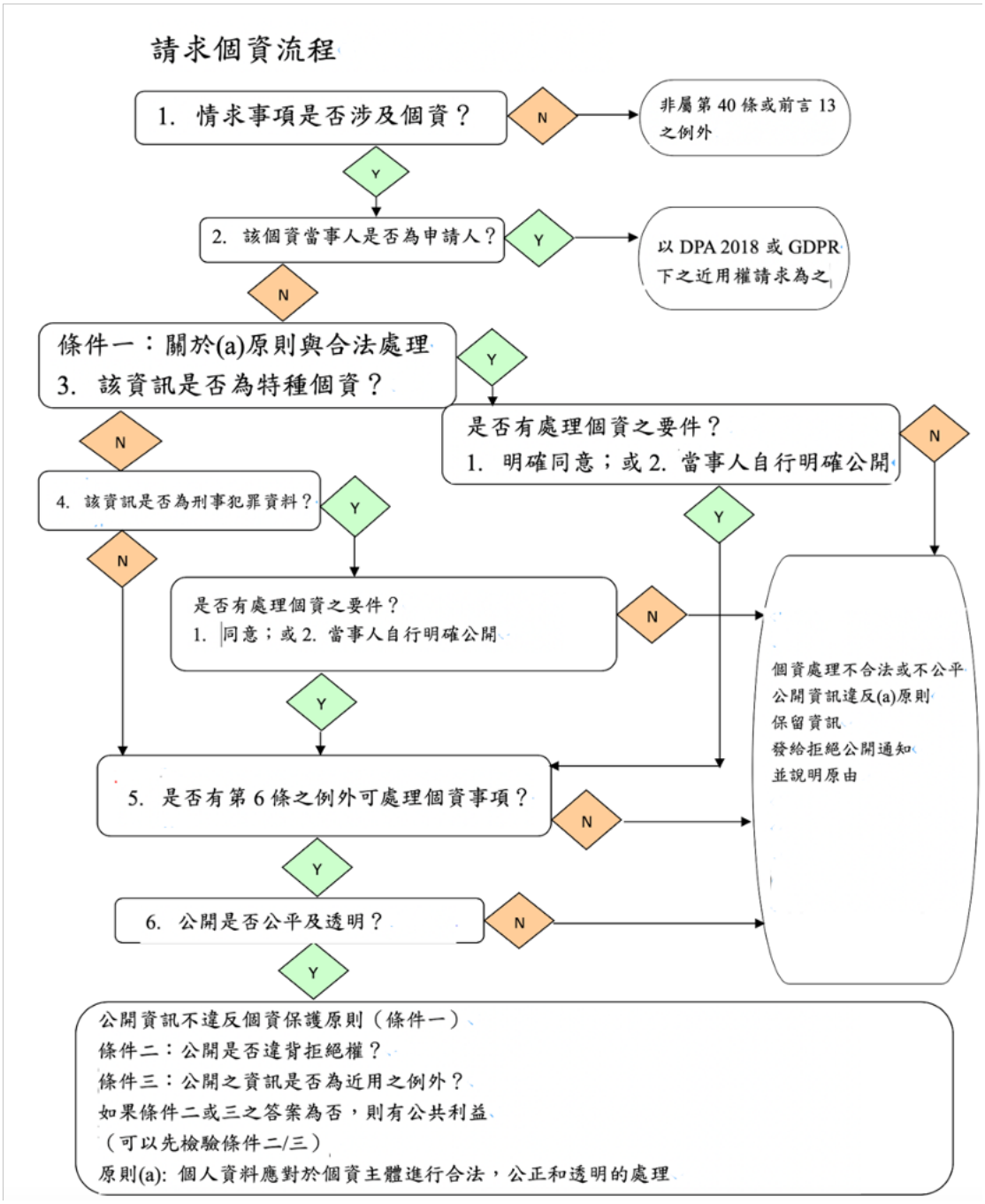
換言之，綜合第三至第五階段，在三種情形下，個資保護可能成為資訊公開之例外：資訊之揭露可能違反個資處理之保護、當事人接近利用要求之例外情狀、或基於公共利益而以不揭露為宜，待相關機關確認資訊係為以上三者後，此時相關機關即無義務對資訊公開之申請人確認或否認其是否有相關之資訊。

---

[118] ICO, Personal information (section 40 and regulation 13), https://ico.org.uk/media/for-organisations/documents/1213/personal-information-section-40-regulation-13.pdf, Version: 2.3, 20190925.

[119] 在該指引中被合併稱為 a 原則。

再者，必須特別強調的是：並不是一定被判定為個人資料或個人隱私事項，即不得公開，而是必須判斷保護的法益之間彼此的衡平[120]。依據該指引，整體判斷流程如下圖[121]：



[120] ICO, Personal information (section 40 and regulation 13), https://ico.org.uk/media/for-organisations/documents/1213/personal-information-section-40-regulation-13.pdf, Version: 2.3, 20190925, 5.
[121] Ibid., 8.

(三) 國家識別代碼之處理（GDPR 第 87 條）

由於英國並無身分證，更無國家之統一識別代碼[122]，因此在 GDPR 將施行之時，資訊委員之衝擊影響與調適報告中便言明並無相關調適[123]。

(四) 僱傭（勞動）關係資料處理（GDPR 第 88 條）

1. 對歐盟層級規範與 GDPR 之解析

在 GDPR 第 88 條關於僱傭關係之個資處理問題規範中，給予會員國一定程度之判斷餘地，可以制定更特定之規則予以保障基本權利與自由。而相關所謂特定規則，事實上 GDPR 允許之態樣包括以法律規範或其他勞資協商 (Collective agreement)之方式，特別是對於例如錄用、工作之環境、衛生與安全事項以及工作之管理事項等加以規範相關個資事項。另外，此處對於基本權利與自由之保障係指尤其是處理之透明、企業團體（法人）之間相互承接流動（例如子、分公司間合併或與母公司之合併等），以及工作時之監控政策等。不過由於 GDPR 允許各會員國各自依照其相關勞動法規予以制定不同規則，因此有論者評論其可能造成保護之落差，尤其在歐盟共同市場人員、服務等四大流通之情況下，不同程度之保護除了或許會造成歐盟內部各會員國之間關於競爭市場之問題以外，不同調的保護標準也可能造成一些實務上難題[124]。

---

122 事實上關於英國之身分證與統一識別證號問題的相關爭議由來已久，詳參：翁逸泓、廖福特，私生活權利：探索歐洲，反思台灣，台北：新學林出版，2014 年 12 月，頁 53-66。

123 ICO, The Information Commissioner's Office (ICO) response to DCMS General Data Protection Regulation (GDPR) derogations call for views, 2017, https://ico.org.uk/media/about-the-ico/consultation-responses/2017/2014036/ico-response-dcms-derogarations-consultation-20170510.pdf, para 130.

124 Carolin Moeller (2017), "Are We Prepared for the 4th Industrial Revolution? Data Protection and Data Security Challenges of Industry 4.0 in the EU Context." In *Data Protection and Privacy: The Age of Intelligent Machines*, edited by Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth and Paul De Hert, 143–166. Computers, Privacy and Data Protection. Oxford: Hart Publishing, 157-159.

首先,關於勞動與僱傭方面之個資保護規範可能散落包括勞動法、通訊傳播法、刑法甚至其他行政規則或是準則類型的軟法(soft law)[125]等各不同法領域規範之間，而可能有一定程度之不明確性、漏洞或是競合矛盾之情狀。例如，德國法上為了避免犯罪發生而監控員工被認定係合於比例原則[126]，但其他歐盟會員國法律可能不盡然如此。

亦有在歐盟層級法律具備較明白規範者,例如在 ePrivacy Directive（電子通訊傳播指令)與後續之 Data Retention Directive(資料留存指令)中即有規定不得監控電子通訊之內容以及其位置資訊等[127]。然而，即便如此，因為該規範僅為指令，因此也有會員國國內法允許監控員工電子郵件者。例如英國在 Halford v UK 與 Copland v UK 兩案中法官表示因為原告並未被預先告知將有監控與介入而有合理隱私期待，但相反地在被預先告知的情況下，則似乎可以因為無合理隱私期待而受一定程度監控或介入。

2. DPA 2018 層面

而英國 DPA 事實上對勞動或僱傭範疇的個資特別豁免或管制事項並未有太多的直接規範，至多能在 DPA 2018 的附件中找到一些線索。例如在附件 2 第 4 部分第 22 點關於（企業/商務）管理預測之規範指出 GDPR 在此不適用關於商業相關之管理行為的預測。ICO 對此舉例：某企業團體資深管理階層預計進行該企業之組織再造，則可能牽涉相關人力調整，因此可能需要處理特定員工之個資，則可能因商業上管理之考量，不使該員工知情該再造計畫，否則對於該計畫生實質上不利之影響[128]。然而，綜觀整個 DPA 2018，事實上並無具有體系性或是特別規範章節乃至條文之勞動隱私特別規範。

---

[125] 即被廣泛接受的行為規範之原則，其性質上無特定的義務要求，近似宣言式聲明。
[126] Ibid, at 158.
[127] 在此規定中，例外可獲得之個資為與帳單相關之資料。
[128] ICO, Exemptions of the GDPR, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex17,

對此，ICO 基於資料保護指令與 GDPR 在此部分之授權，但英國國內法尚未有具體規範之現況，早在 2011 年便有僱傭實務準則(the employment practices code)[129]，分別就重要事項如應徵與選才(Recruitment and selection)、僱傭紀錄(Employment records)、工作監管(Monitoring at work)與勞動者健康狀況(Information about workers' health)等加以說明。

例如，在該準則中就應徵與選才部分，指出如果資料控管者蒐集或處理個資以作為人才甄選之用，例如要求填寫履歷表或郵寄、上傳履歷等，即適用 DPA。適用 DPA 之結果並不妨礙選才之效率，而是衡平雇用人所需資訊與受雇人私生活權利與隱私保障，而最重要者，應屬透明與公開原則，即使應徵人知道其個資之流向與應用，而毫無保留的要求應徵者個資，也為 DPA 所不許[130]，而同樣之原則也幾乎都是用在其他的勞僱情狀。在此，較為重要者係如果雇主希望得到應徵者犯罪紀錄，只能申請犯罪紀錄署(Criminal Records Bureau, CRB)之揭露。

附帶一提，在歐洲人權法院 *Niemietz v Germany* 案判決中，法院認為在工作環境中，勞動者仍有一定程度之個人隱私需被保護，但事實上法院也認為在工作環境中對於個人隱私事項與專業上的公務/商務事項很難具體清楚地劃分，故需要平衡勞資雙方對隱私之期待與工作環境之安全與品質監控。再者，於歐洲人權法院 *Bărbulescu v. Romania* 案中，法院也認為對於監看員工之電子通訊，雖然在工作環境中對於個人隱私事項與專業上的公務/商務事項很難具體清楚地劃分，但是在程序上雇主召集員工解釋其使用公司資源，特別是網路的使用與相關政策時，必須實際上確認該員工是否已經接近使用了有關說明文件的

[129] ICO, the employment practices code, https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf ,

[130] ICO, Quick guide to the employment practices code, https://ico.org.uk/media/for-organisations/documents/1128/quick_guide_to_the_employment_practices_code.pdf, 6.

內容，並在基於監看而要對員工進行紀律處分時，必須在每個階段都確保文件被員工近用，並保持透明性原則：說明在哪些情況下員工將被監看、告知員工相關監視的性質或程度的事實、考慮到侵入員工的私人生活和通信的程度、確定首先要採取監測措施的具體原因。另外，在實際監看上，雇主也需考量是否可以採取措施減少對其員工的私人生活和通訊的侵犯，也需確認雇主是否可能在員工不知情的情況下近用了員工的通訊[131]。

(五) 基於公益之檔案儲存目的、基於學術或歷史研究目的以及統計目的之處理（GDPR 第 89 條）

GDPR 第 89 條所指相關例外規定，本報告在此之前已經在關於 GDPR 第 85 條之說明處，說明了與 89 條之區別實益。除前述相關區別與要件之外，GDPR 第 89 條的科學與歷史為目的之研究特權，事實上還包含其他例外地允許處理個資事由：

- 作為特種個資之例外允許處理情狀[132]；
- 於第三人獲得個資時，關於透明原則義務要求之減緩；
- 個資留存期間限制之延展；以及
- 作為豁免資料控管者責任之事由。

於英國 DPA 2018 對應規範在第 19 條，第 1 項將範圍釐清於公共利益為目的建檔(archiving)之必要、科學與歷史研究目的之必要、以及統計目的之必要等三類型。第 2 項規定雖這些類型個資之處理符合 GDPR 第 89 條第 1 項之要件，但如對於當事人會造成實質傷害或實質侵擾時，則不得為之。第 3 項規定如果出於針對特定當事人的措施或決策的目的而進行個資處理，則除非必要的處理目的包括批准的醫學研究的目的，否則此類處理並非滿足 GDPR 第 89 條之要求。第 4 項則

[131] 因為歐盟法院就人權事項大多「尊重」歐洲人權法院之判決意見，又個資保護事項與隱私權被歐盟人權憲章寫入其第 7、8 條，故事實上具相當參考價值與依據。
[132] Article 9(2)(j), GDPR.

定義何謂醫學研究(medical research)以及何謂 NHS 相關單位，第 5 項則規定國務卿得經由第 6 項之程序修正前述醫學研究之定義。

而於特種資料之禁止處理時，如要享有 DPA 2018 第 19 條之豁免，必須合於附件 1 第 4 點之條件，也就是必須合理且符合比例（必要性原則之檢驗），並符合公共利益。而公共利益雖在此未明文，ICO 仍指出必須將該等公共利益予以明確化，且必須係為整體社會之「公共」利益，而非特定個人（如研究者）之利益（如純粹學術研究興趣）[133]。

DPA 2018 另外在附件 2 第 6 部分第 27、28 點規範有 GDPR 相關調和之權利如將阻止或嚴重損害實現個資處理目的時，則不適用關於歷史、科學研究與統計建檔目的之調和規定（Sec. 27(1)與 Sec. 28(1)），並區分為排除 GDPR 之適用（Sec. 27(2)[134]與 Sec. 28(2)[135]）或豁免責任（Sec. 27(3)[136]與 Sec. 28(3)[137]）二種類型。

---

[133] ICO, What are the conditions for processing?, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions10.

[134] (2) For the purposes of this paragraph, the listed GDPR provisions are the following provisions of the GDPR (the rights in which may be derogated from by virtue of Article 89(2) of the GDPR)—
(a)Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);
(b)Article 16 (right to rectification);
(c)Article 18(1) (restriction of processing);
(d)Article 21(1) (objections to processing).

[135] (2) For the purposes of this paragraph, the listed GDPR provisions are the following provisions of the GDPR (the rights in which may be derogated from by virtue of Article 89(3) of the GDPR)—
(a)Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);
(b)Article 16 (right to rectification);
(c)Article 18(1) (restriction of processing);
(d)Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);
(e)Article 20(1) (right to data portability);
(f)Article 21(1) (objections to processing).

[136] (3) The exemption in sub-paragraph (1) is available only where—
(a)the personal data is processed in accordance with Article 89(1) of the GDPR (as supplemented by section 19), and
(b)as regards the disapplication of Article 15(1) to (3), the results of the research or any resulting statistics are not made available in a form which identifies a data subject.

細究之，依據前述於競合時之調和（包括限制當事人權利或是增加資料控管者、受託處理者義務之規定）情狀，當事人權利類型於基於學術或歷史研究目的之情況如下[138]：

- GDPR 第 15 條（近用權）：雖 GDPR 未予調和，但 DPA 2018 之排除條款規範如將阻止或嚴重損害實現個資處理目的時，不適用限制當事人權利或是增加個資控管者、受託處理者義務之相關調和規範。
- GDPR 第 16 條（更正權）：雖 GDPR 未予調和，但 DPA 2018 之排除條款規範如將阻止或嚴重損害實現個資處理目的時，不適用調和。
- GDPR 第 17 條（刪除權、被遺忘權）：GDPR 規範如對於當事人會造成實質傷害或實質侵擾時，則不得為之。DPA 2018 依循 GDPR，本身無另外規範。
- GDPR 第 18 條（限制處理權）：GDPR 規範只允許在當事人同意或是基於重大公共利益時得為個資處理；DPA 2018 之排除條款規範如將阻止或嚴重損害實現個資處理目的時，不適用調和。
- GDPR 第 19 條（控管者更正、刪除或限制處理之通知義務）：在 GDPR 規範除非該等通知是不可能或是需要不成比例的勞力方例外地不需要通知；但 DPA 2018 之排除條款規範僅限於以統計為目的之處理時[139]，如將阻止或嚴重損害實現個資處理目的時，不適用調和。
- GDPR 第 20 條（資料可攜權）：資料可攜權在 GDPR 之下僅有當事人同意之情況下可以行使；但 DPA 2018 之排除條款規範

---

[137] (3)The exemption in sub-paragraph (1) is available only where the personal data is processed in accordance with Article 89(1) of the GDPR (as supplemented by section 19).

[138] See: Miranda Mourby, Heather Gowans, Stergios Aidinlis, Hannah Smith, Jane Kaye, 203-204.

[139] GDPR 第 89 條第 3 項就 GDPR 第 19 條給予會員國排除適用餘地，英國 DPA 在附件 2 第 6 部分第 28(d)點僅排除以統計建檔為目的之處理。

僅限於以統計為目的之處理時[140]，如將阻止或嚴重損害實現個資處理目的時，不適用調和。

- GDPR 第 21 條（拒絕權）：GDPR 僅限於為公共利益之必要而為研究時，調和當事人拒絕權（使之不得拒絕）；DPA 2018 之排除條款規範如將阻止或嚴重損害實現個資處理目的時，不適用調和。
- GDPR 第 22 條（對自動處理、剖析與據以決策之拒絕權）：在 GDPR 之規定下，僅有歐盟法或會員國本國法規範時可調和，但 DPA 2018 無相關排除規範。

五、 自動化機器做成之決定

(一) 對歐盟層級規範與 GDPR 之解析

人工智慧的應用在近來科技發展潮流下，係為重要研究方向與商業化利用趨勢。事實上對於人工智慧技術發展應用對法律以及社會、倫理之衝擊與對策，歐盟在 2019 年 4 月邀請各界代表組成人工智慧高級顧問團，發佈「可信賴的人工智慧道德指引(Ethics Guidelines for Trusted AI)」[141]，其中三個貫穿整個指引的基本要素乃係：首需合法，其次要合乎道德，最後必須要「穩健(robust)」[142]。而該指引臚列七大原則，作為未來人工智慧發展的重要基石：

1. 人類主體和監督：人工智慧系統應賦權(empower)予人類，使其能做出明智的決定並促進其基本權利。同時，需要確保適當的監督機制，這可以透過「需要人為交流的模型(Human-in-the-loop)」[143]，

[140] GDPR 第 89 條第 3 項就 GDPR 第 20(1)條給予會員國排除適用餘地，英國 DPA 在附件 2 第 6 部分第 28(d)點僅排除以統計建檔為目的之處理。

[141] EU High-Level Expert Group on AI , Ethics Guidelines for Trustworthy Artificial Intelligence , https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419, 8 April 2019

[142] Ibid., 5.

[143] 指在系統的每個決策週期中進行人為干預的能力，在許多情況下這是不可能的，也不是所希望的。Ibid., 18.

「人在循環模型之上(Human-on-the-loop)」[144]和「人類發出命令(Human in Command) 」[145]的方法來實現。

2. 技術的穩健性和安全性：AI 系統必須具有彈性和安全性。他們需要安全，確保在發生問題時進行後援計劃，並且要準確，可靠和可重複。這是確保最大程度地減少和防止意外傷害的唯一方法。
3. 隱私和資料治理：除了確保完全尊重隱私和資料保護外，還必須確保充分的資料治理機制，同時考慮到資料的質量和完整性，並確保對資料的合法近用。
4. 透明度：資料、系統和 AI 商業業務模型應透明，而可追溯性機制可以幫助實現這一目標。此外，人工智慧系統及其決策應以適合相關利益相關者的方式進行解釋。人們需要意識到自己正在與 AI 系統進行交流，並且必須了解系統的功能和局限性。
5. 多樣性、禁止歧視和維持公正：人工智慧必須避免不公正的偏見，因為它可能產生多種負面影響，包含了從弱勢群體的邊緣化到偏見和歧視的加劇。為了促進多樣性，因此無論其是否有身心障礙，人工智慧系統均應該為所有人提供便利，並在其整個生命週期中讓利益相關者參與。
6. 社會和環境福祉：人工智慧系統應使全人類包括後代受益。因此，必須確保它們是可持續的和友好環境的。此外，人工智慧系統應考慮到環境，包括其他生物，並應認真考慮其社會和社會影響。
7. 課責制：應建立機制以確保對人工智慧系統及其結果的責任和課責制。

其中可以發現以個人資料作為最大宗驅動動力來源的人工智慧系統應用，在許多面向上其核心原則與個人資料保護之核心原則，多有重疊，因此 GDPR 相關規範，尤其是本節所要討論的以機器自動化做成決策問題，有密切關聯。

---

[144] 在系統設計週期中進行人工干預並監視系統運行的能力。Ibid., 18.

[145] 監督 AI 系統整體活動（包括其更廣泛的經濟、社會、法律和道德影響）的能力。Ibid., 18.

須注意者，剖析僅為以機器自動化處理、利用個人資料後所做成之評價，而該等評價可以作為至少三種不同功能之利用：找出當事人偏好、預測當事人行為，以及可作為進一步決策之依據，在此，只有第三種作為決策之依據的態樣，會使得剖析成為自動化做成決策之一部分。須注意者，此二者於決定之作成係由一系列之機器對於個人資料作出處理、利用而後逕為決定之時，可能有所重疊，而非必為絕對分離之概念。

關於此處之以機器對個人自動化作成決策與個人資料保護之問題，歐盟資料保護指令早在 1995 年即明文規範有當事人應有權不受自動化決策之拘束（not to be subject to a decision）[146]，而該決策需對當事人產生法律效果或類似之重大影響，並僅以自動化處理來評估其個人特徵之措施。例如：網路簽證申請之自動否准，或不包括任何人為介入之電子化人力招募等。依指令及其解釋，即便為締結或履行當事人與控管者間之契約所必須，或當事人已明確同意，資料控管者仍應執行歐盟或會員國規範之適當措施，以保護當事人之權利及自由及正當利益，並至少應確保得以部分之人為參與（human intervention）、表達意見（to express his or her point of view）及獲得挑戰該決定（contest the decision）之機會[147]，此項權利亦繼續被規範在 GDPR 第 22 條第 1 項拒絕機器自動化決策權。[148]

本報告就體系解釋言，就此部分認為或可將該等權利解釋為拒絕權。第 22 條關於（以機器）對個人自動化決策，包含剖析的相關規定，在體系上是位於關於當事人權利保障體系下，第四節「拒絕權及對個

---

[146] 歐盟資料保護指令第 15 條參照。

[147] Lee A. Bygrave, *Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, 17 COMPUTER LAW & SECURITY REPORT 17, 18-21 (2001).

[148] 在劉靜怡教授的卓文中也曾就此問題提出爭點整理，認為未來對於第 22 條應該禁止說或是「有權反對」說做出判斷，係為相關爭議問題之研究重點。劉靜怡，〈人工智慧潛在倫理與法律議題鳥瞰與初步分析—從責任分配到市場競爭〉，載於：劉靜怡編，《人工智慧相關法律議題芻議》，元照出版，2018 年 11 月，頁 43。

人之自動化決策，包含剖析(Automated individual decision-making, including profiling)」涵括了兩個重要規範，其一是第 21 條的拒絕權，其二是第 22 條對個人自動化決策，包含剖析之規範，而這二者被放在同一小節之內，顯見其在體系上應為不相互排斥且彼此支持之解釋。

第 22 條第 1 項指出如果當事人不拒絕第 21 條第 5 項「以使用技術規範/標準的自動化處理（個人資料）」而導致該等自動化處理產生決策時，在邏輯上應該被賦予對「（以機器）自動化作成決策」並在法律上發生效果或類似之重大影響結果出現時的拒絕權：[149]當事人應有權不受僅基於自動化處理（包括剖析）所做成而對其產生法律效果或類似之重大影響之決策所拘束。關於此拒絕權之內涵[150]說明如下：

1. 法律效果或類似之重大影響結果

GDPR 本身並未詳細定義何謂「類似之重大影響結果」，至多可以在其前言第 71 點找到例子：例如網路信用貸款申請時，因為信用評價負評而產生之自動拒絕，或不包括任何人為介入之電子化人力招募。又或著從第 22 條第 2 項推論出的基於對個人自動化決策生成的締結契約行為。

另外，文獻上亦提出其他舉例，例如投放廣告(targeted advertisement)是否即為所謂類似之重大結果。基於投放廣告之結果未必立即造成如同 GDPR 前言舉的例子一樣生成拒絕放貸、拒絕聘用或

[149] 就此處 right to object 之相關權利言，在解釋上向來有關於此處係為「禁止」傾向保護當事人利益，或是「有權反對」之防禦，而傾向維護資料控管者之權利，一向有所爭論。本報告在英國部分作者較傾向前者，本報告在德國部分相關介紹時，則以抵禦之權利說明。事實上在學說上仍未有定論，相關之辯論詳參：Bygrave, Lee Andrew (2020). Article 22: Automated individual decision-making, including profiling, In Christopher Kuner; Lee Andrew Bygrave & Christopher Docksey (ed.), The EU General Data Protection Regulation (GDPR): A Commentary, 530-532.基於本報告雖盡量希望能統整論述，惟為避免與個別作者之學說一貫性論述發生矛盾，仍採分別立場，並以此為註。

[150] 相關的說明與解釋，亦可參考：劉靜怡，〈人工智慧潛在倫理與法律議題鳥瞰與初步分析—從責任分配到市場競爭〉，載於：劉靜怡編，《人工智慧相關法律議題芻議》，元照出版，2018 年 11 月，頁 36-43。

是締結契約的法律效果，因此恐怕不能說是適合的情狀[151]。不過，當投放廣告造成對於特定相對人提供不同待遇時，仍應該被認定是此處之類似法律效力的重大結果。本報告認為，在此，考量之點有二：其一，是否產生差別對待之結果；其二，發生了壟斷資訊之結果。前者的原因是因為該等決策結果可能是基於一個具有偏見或歧視的演算法（而這點在發展人工智慧應用時，被歐盟列為重大核心原則如前述），或是結果之誤差；後者則是基於對資訊的壟斷將形成當事人基於資訊之缺乏而產生不對稱之決策結果。而包括避免偏見或歧視、提供一個合適的數學或統計程序以避免誤差等，均在 GDPR 前言例如第 71 點，可尋得論理依據。

2. 例外情狀

如果以自動化（包括人工智慧）方式影響當事人法律上權利，則在 GDPR 第 22 條第 2 項下一般之個資僅有三種情狀可例外地被允許，也就是在符合個資保護的基本原則後：(1)締結或履行控管者與個人之契約所必要；(2)控管者受拘束之會員國或歐盟法律有明文授權，且定有適當保護當事人權利及自由與正當利益之措施；以及(3)基於當事人明確同意者。但如果自動化做成之決策含有特種個資，則第 22 條第 4 項規範僅限於必須當事人明確同意或是個資之處理（自動化做成決策）係為實質公共利益必要之所需，並且遵從個資保護核心且以適當及特定之措施保障當事人基本權利與利益。

比較值得注意而與本報告有直接關連的在於第二個例外，事實上似乎開啟了給予會員國立法之空白授權。不過在解釋上，仍然可以回到 GDPR 前言第 71 點找尋線索：舉例而言，例外之情況包括為監控、預防詐騙，及逃漏稅之目的。另方面，在實務上較常出現基於當事人之明確同意作為此處例外的例子，大多出現在保險契約相關的評估風

[151] Joachim Schrey, General Condictiones for Data Processing in Companies under the GDPR, in Daniel Rücker and Tobias Kugler Ed. (2017), New European General Data Protection Regulation: A Practitioner's Guide, Nomos/Hart, 149-150.

險條款中。[152]

至於就第一個與第三個例外而言，則主要爭點則在當事人之審查權(right to review) [153]。這個審查權之概念，劉靜怡教授將其視為係「自動化決策解釋權(right to explanation)」其中的一個規範基礎，規範了關於防衛的概念，出現在第 22 條第 3 項[154]之規範：「資料控管者應執行適當保護措施以確保當事人之權利及自由及正當利益，至少有權對控管者部分為人為參與、表達意見以及挑戰該決策」之中。據此，該「防衛權」至少包括使得當事人有「取得人為介入權(right to obtain human intervention)」、「(對自動化決策）表示意見權」，以及「挑戰決策權」。

關於 GDPR 第 22 條第 2 項對個人自動化決策之例外的最後一個問題，則是在 GDPR 第 70 條第 1 項第 f 款中規範：為進一步規範根據第 22 條第 2 項剖析之標準與條件，(會員國之個資獨立專責主管機關）需依本項第 e 款點發布指導原則、建議及最佳做法。而 GDPR 第 70 條第 1 項第 e 款則規範了各會員國專責機關的任務之一：(其需）主動或依其一名成員或歐盟執委會之請求，審查涵蓋本規則(GDPR)適用之任何問題並發布指導原則、建議及最佳實踐以鼓勵GDPR之一體適用。據此，本報告以下觀察並分析在英國之法律規範與實踐。

(二) GDPR 關於此部分在英國之落實

英國 2018 年 DPA 亦配合 GDPR 第 22 條規定，制定相應國內規範，改變 1998 年資料保護法原則上容許資料自動化決策而僅於重大影響時通知當事人之規定。

---

[152] Joachim Schrey, General Condictiones for Data Processing in Companies under the GDPR, in Daniel Rücker and Tobias Kugler Ed. (2017), New European General Data Protection Regulation: A Practitioner's Guide, Nomos/Hart, 150-151.

[153] Joachim Schrey, General Condictiones for Data Processing in Companies under the GDPR, in Daniel Rücker and Tobias Kugler Ed. (2017), New European General Data Protection Regulation: A Practitioner's Guide, Nomos/Hart, 151.

[154] 劉靜怡，〈人工智慧潛在倫理與法律議題鳥瞰與初步分析—從責任分配到市場競爭〉，載於：劉靜怡編，《人工智慧相關法律議題芻議》，元照出版，2018 年 11 月，頁 40-41。

DPA 2018 首先在對 GDPR 相關授權會員國決定事項（評斷餘地）之部分，於第 14 條規範了法律授權的自動化決策與相關保障措施，並在第 1 項說明該條文係為 GDPR 第 22 條第 2 項第 b 款的目的而做的國內立法規定，此相關立法規範是 GDPR 第 22 條第 1 項的例外。DPA 2018 第 14 條第 2 項則定義何謂 GDPR 第 22 條第 1 項中尚未具體定義的「重大決策(significant decisions)」：對當事人產生法律效果，或同樣顯著地影響當事人。然而，這個定義事實上仍與 GDPR 第 22 條第 1 項有著相同的模糊性與不明確性。因此 DPA 2018 第 14 條第 3 項規範有「準重大決策(qualifying significant decision)」之要件：係與當事人有關的重大決策，且是法律要求或授權的，但不屬於 GDPR 第 22 條第 2 項第 a 款或第 c 款，也就是非為契約必需的決策或在當事人同意的情況下做出的決策。

而前述要件成就以後，其法律效果為如若資料控管者僅基於自動化處理就對當事人之準重大決策，則：(a)資料控管者必須在合理可行的範圍內，盡快地以書面通知當事人該僅基於自動處理已做出的決策，並且(b)當事人得於收到通知起 1 個月期間內，請求資料控管者重新考慮該決策，或做出不完全基於自動化處理的新決策。資料控管者基於 DPA 第 14 條第 5 項之規定，對當事人前述之請求，則必須在期間內(a)考量該請求，而考量之點包括當事人提供的與其相關的任何資訊；(b)完成請求；及(c)以書面通知將包括為符合請求而採取的步驟，以及完成請求的結果等事項，通知當事人。最後，國務卿對前述 GDPR 授權會員國裁量之立法空間，可以基於保障當事人基本權利與自由之本質，透過正當程序予以修正。相關之規定也被規範在 DPA 2018 第 49 條及第 50 條關於當事人之保障中，以及 DPA 2018 關於國安情報處理個資的第 96 條及第 97 條中。

2018 年 ICO 就 GDPR 有關對資料自動化決策與資料剖析之規定，公布了細部指引(detailed guidance on automated decision-making and

profiling)[155]，供企業、組織參考。在現今的 GDPR 規範下關於自動化做成決策之個資保護所謂的適當保護措施，英國資訊委員認為必須至少符合幾個要件：告知當事人關於其個資處理之相關資訊、導入易於人為介入或挑戰（例如申訴或異議等行為）決策過程之機制，以及持續確保該系統如預期目的運作[156]。根據指導文件，DPA 2018 與 DPA 1998 在此部分最大的不同是因應 GDPR 之修正，當事人有權利發出通知，請求資料控管者不要使用其個人資料做出任何自動化決策；並要求資料控管者重新考慮通過自動化方式做出的決定[157]。

相對地，資料控管者僅在訂立或履行契約所必需、由歐盟或會員國法律授權，或基於個人的明確同意時，方得為 GDPR 第 22 條第 1 項之行為。並且資料控管者新增責任包括：主動告知當事人有關剖析和自動化決策的資訊；進行此類處理時，需採取適當的防護措施；以及對當事人說明個人行使相關權利的程序。另外，其他特別限制則適用於特種個資和涉及兒童的自動化決策[158]。

ICO 也特別指出企業、組織為因應 GDPR 而需特別留意或做出改變的事項包括了[159]:

1. 記錄資料處理活動，以幫助確認資料處理是否符合 GDPR 第 22 條第 1 項關於剖析與自動化決策之定義。
2. 倘資料處理涉及資料剖析或重大自動化決策，應進行個資保護影響評估(DPIA)，以判斷是否有 GDPR 第 22 條之適用，並及

[155] ICO, Automated decision-making and profiling, 2018/06/05, https://ico.org.uk/about-the-ico/news-and-events/ai-blog-automated-decision-making-the-role-of-meaningful-human-reviews/.

[156] Information Commissioner's Office, *Rights Related to Automated Decision Making Including Profiling*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/ (last visited Jul. 31, 2019).

[157] Ibid., 4-5.

[158] Ibid., 4.

[159] Ibid., 5.

早了解相關處理個資之風險以便因應。

3. 提供給當事人的隱私權資訊(privacy information)，必須包含自動化決策相關特別細部之資訊。
4. 應確保組織有相關程序能接受當事人的申訴或異議，並有獨立審查機制。

細部指引並解釋所謂「僅以自動化決策」[160]、「資料剖析」[161]、「有法律效果或類似重大影響」[162]之意義，另就可進行單純自動化決策的三種例外情況簡單舉例。這三個例外狀況包含：[163]

1. 個人或家庭活動：在純粹的個人或家庭活動過程中處理個人資料而與專業或商業活動無關者，因為不在 GDPR 的範圍內，故當然可進行單純自動化決策。
2. 執行法律：主管機關基於執法目的處理個人資料亦不在 GDPR 的範圍內（例如，警方調查犯罪），相反地，此類處理應遵循 DPA 2018 第 3 部分中的規則。並且，Law Enforcement Directive 第 11 條第 1 項則規範有經資料控管者受拘束之歐盟法或會員國法授權，且為該當事人之權利與自由提供適當安全保護措施者（至少有權對資料控管者部分為人為介入），不在此限。
3. 國家安全：為維護國家安全或國防目的而處理的個人資料不在 GDPR 的範圍內。換言之，雖然事實上 DPA 2018 關於 GDPR 之適用的第 3 章第 2 部分涵蓋了該內容，其中亦包含對國家安全和國防的豁免。

---

[160] ICO 舉例，例如工廠工人的工資與他們的生產率相關聯，而該生產率會自動受到監控。透過參考所蒐集的有關其生產率的資料，可以自動確定工人在每個工作班次中所獲得的報酬。Ibid., 10.

[161] 例如資料控管者可以了解有關個人偏好的信息；預測他們的行為；和/或做出有關他們的決定。Ibid., 6.

[162] 例如從政府補貼所獲得的數額可能會影響一個人的生計或購買、租賃房屋的能力，因此該決定也會產生「類似的重大影響」。或是個人線上申請貸款，而該網站使用演算法和自動信用搜尋來對應用程序做出即時的允、否判定。Ibid., 10-11.

[163] Ibid., 275.

此外，縱使符合例外情況得進行僅以自動化決策，資料控管者仍必須提供有意義之重要資訊(meaningful information)給當事人，包括使用個人資料與自動化決策邏輯上的關聯性、對當事人可能產生的結果。而對所謂類似重大影響，ICO 提出如果不確定某個決策是否會對某人產生類似的重大影響，則應考慮該決定可能對其產生的影響作為判斷參考，例如：財務狀況、健康、聲譽、就業機會、行為或選擇[164]。

細部指引在關於資當事人之審查權(right to review)/自動化決策解釋權(right to explanation)就其有權向控管者「表達意見」部分，說明控管者對此應至少回應包括自動化決策是為何以及如何達致該決策結果，也因此控管者必須確認該決策結果，並以簡單的舉例來解釋決策背後之邏輯。此外，因為資料控管者需要回覆當事人此項權利，所以資料控管者所使用的系統應該要能提供監理控管與追蹤功能，以顯示構成決策基礎的關鍵決策點。如無法為之，則需要使當事人了解為什麼不選擇該等功能[165]。

又，為了回應審查權中關於「挑戰」決策之事項，資料控管者應該有一個針對個人的質疑或申訴決定的程序，以及可以提出申訴的管道。另外，資料控管者還應確保任何審查均由具有適當資格並有權更改決定的人員進行。前述之有權更改決定之人，應考慮該決定所依據的原始事實，以及該當事人可以提供來支持其挑戰的任何其他證據[166]。

六、 當事人權利

(一) 英國 DPA 2018 限縮 GDPR 有關當事人權利行使

GDPR 第 23 條賦予會員國一定之調整空間，得以內國法限縮 GDPR

[164] Ibid., 18.
[165] Ibid., 19.
[166] Ibid.

所規範當事人權利相關之適用要件。對此，英國 DPA 2018 於附件 2 第 3 部分與第 4 部分加以限縮權利之適用要件，即保護他人權利，以及基於規範 GDPR 第 13 條及第 14 條之告知義務、第 15 條之近用權，並鬆綁前述三個條文對應在 GDPR 第 5 條第 a 款至第 c 款之相關原則。[167]

此間，有關上開後者，英國 DPA 2018 附件 2 第 4 部分第 19 條排除含有法律專業事務，使得法律專業在訴訟相關程序上，享有特權；第 20 條規範關於自證己罪之當事人權利問題，亦即在法院審理中或在法院審理前藉由陳述等表明自己與某一犯罪有關或將使自己受到刑事指控的行為時，任何人無須遵守上開英國 DPA 2018 附件 2 第 4 部分第 18 條所列的 GDPR 規定(下稱所列 GDPR 規定)，只要其遵守程度會通過揭示犯罪的證據而使該人面臨該罪行的訴訟程序即可。第 21 條規範關於公司財務，使得所列 GDPR 規定不適用於在滿足條件 A 或條件 B 的情況下為相關人員提供的公司財務服務或與之相關的已處理個人資料。條件 A 是所列 GDPR 規定的應用可能會影響某（金融）工具（即貨幣或對應替代之憑證）的價格。

條件 B 為相關主體合理地認為，將所列 GDPR 規定應用於相關個人資料可能會影響以下個人的決定（第 21 條第 3 項參照）：

1.是否買賣、認購或發行票據/ 憑證，或 2.是否以可能對商業活動產生影響的方式行事（例如，對個人的產業戰略，企業的資本結構或企業或資產的法定或實質所有權產生影響），和 GDPR 規定應用於該個人資料將對金融市場的有序運行或經濟體內資本的有效分配產生不利影響。

第 22 條規範管理預測，明訂所列 GDPR 規定只要這些規定的應用可能會損害業務或活動的進行之虞，則不適用於基於與業務或其他活動有關的管理預測或管理計劃目的而處理的個人資料。第 23 條規範協

[167] DPA 2018 附件 2 第 4 部分第 18 條參照。

商（契約法上之磋商過程），明訂所列 GDPR 規定不適用於個人資料包含資料控管者意圖與當事人進行協商之記錄，但前提是該等規定的應用可能會損害這些談判方有適用。

第 24 條調和秘密參考來源，對此所列 GDPR 規定不適用於出於以下目的而秘密提供的（或將要提供的）參考資料所構成的個人資料：（a）對當事人的教育，培訓或就業（或預期教育，培訓或就業）；（b）當事人作為志願者（或預期作為）；（c）當事人作為對任何機構官員任命（或預期的任命）；或（d）任何服務提供（或預期提供）。最後，第 25 條則針對考試題目與分數，做出豁免控管者義務規定。

(二) 兒童權利保護

關於兒童權利保護於 GDPR 及 DPA 2018 之個資規範問題，首先必須處理的前提是關於「兒童」之定義。事實上，雖然 GDPR 並未直接定義兒童，但是 ICO 指出[168]依據「聯合國兒童權利公約」(United Nations Convention on the Rights of the Child)之規定[169]，18 歲以下之人皆為「兒童」，而基於所有歐盟會員國皆簽署與批准該公約（第 1 條）[170]，英國自然也如此。

1. 對歐盟層級規範與 GDPR 之解析

比較特殊的是 GDPR 相較於原本資料保護指令不同之規定，即其第 8 條在涉及資訊社會服務(Information Social Service, ISS)時，關於對兒童適用同意之要件，也就是第 1 項後段所指如兒童未滿 16 歲，僅限於其法定代理人授權或是同意之範圍內，其個資之處理方為合法。這

[168] ICO, Children and the GDPR, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/,

[169] UN General Assembly, Convention on the Rights of the Child, 20 November 1989, United Nations, Treaty Series, vol. 1577, p. 3.

[170] Article 1: a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.

是因為兒童或許無法理解個資相關的風險、後果以及保護措施及使用者處理個人資料相關權利，故 GDPR 在前言即說明需要有特殊保護(specific protection) [171]。因此，特別是若所蒐集之兒童個人資料將用於行銷或建立用戶檔案等特定目的，或是會直接向兒童提供服務，而需蒐集兒童相關個人資料之情況，應有特殊保護。而關於這個 16 歲之規定，可見其適用之範圍係對於兒童提供「資訊社會服務」。

至此，即必須對 ISS 加以定義。事實上 ISS 此名詞係來自於歐盟關於技術規則與資訊社會服務領域相關資訊之程序指令[172]第 1(1)(b)條之定義：通常以一定距離，通過電子方式並應服務接受者的個人要求提供有償服務的任何服務[173]。此時所指「一定距離」，即提供服務時各方沒有同時出席；透過「電子方式」，指該服務最初是通過電子設備發送和接收之用於處理（包括數位壓縮）和資料的電子設備，並且通過有線、無線電、光學手段或其他電磁方式完全傳輸，傳送和接收；「應服務接受者的個人要求提供有償服務」則指通過根據個人要求傳輸資料來提供服務。據此，從本質上來說大多數線上服務都會落在 ISS 的定義範圍內，即便該服務的「報酬」或資金並非直接來自最終用戶，也會被認定為 ISS。ICO 舉例，例如向最終使用者免費提供但通過廣告資助的線上遊戲應用程序或搜索引擎，仍屬於 ISS 的定義範疇內[174]。

不過，基於 GDPR 第 8 條第 1 項也同時規定會員國得另以法律規定對兒童提供 ISS 須法定代理人授權或同意之最低年齡，英國對此在 DPA 2018 第 9 條將年齡降到 13 歲（GDPR 准許之最低年限），ISS 之定義範圍則排除線上之預防或諮詢服務。

---

[171] Recital 38 of the GDPR.

[172] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.

[173] 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.'

[174] ICO, Children and the GDPR, https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf, 23.

ICO 在其關於兒童權利與 GDPR 關係的說明中，尤其是與資料保護指令的不同之處[175]，也提醒 GDPR 在前言說明由於兒童需要特別保護，因此當涉及兒童資料處理時，任何資訊或溝通，均應以兒童可以清楚理解的簡易語言呈現[176]。以符合 GDPR 第 12 條第 1 項規定：「控管者應採取適當措施，以簡明、透明、易懂且方便取得之格式，並採用清楚簡易之語言，提供第 13 條及第 14 條所定任何資訊及第 15 條至第 22 條及第 34 條所定關於對當事人所為處理之任何溝通，特別是對於兒童之資訊。該資訊應以書面或其他方式提供，包括於適當情況下之電子格式。當當事人提出要求，並以其他方式確認當事人之身分者，得以口頭提供資訊。」

ICO 提到 GDPR 其他對於兒童特別保護的差異點在於若所蒐集之兒童個人資料將用於行銷或建立用戶檔案等特定目的，或是直接向兒童提供服務，而需蒐集兒童相關個人資之情況下，應有特殊保護。

又，GDPR 也指出除非有相對合適之方法以保障兒童之基本權利與自由，否則如果處理個資之行為對他們有法律效果或類似的重大影響的話，則不應讓兒童接受自動處理（包括剖析）的決策[177]。

最後，ICO 指出 GDPR 要求對兒童個資須特別保護的策略需考量比以往資料保護指令時代更周延：GDPR 要求對兒童為相關通知時應以適合該等年齡之方式為之，例如前述須以平易之語言溝通；基於同意而得蒐集兒童個資時，更應特別考量其刪除權之行使。ICO 也特別指出在蒐集兒童個資時，總括而言，應該考慮有必要從一開始就特別保護他們，並需牢記以此考量來設計處理個資之系統和流程。

2. DPA 2018 層面

[175] ICO, Children and the GDPR, https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf, 9.
[176] Recital 58 of the GDPR.
[177] Recital 71 of the GDPR.

比較特別的是，DPA 2018 為此在第 123 條特別規範要求資訊委員必須加以準備「適合年齡設計準則(Age-appropriate design code)」。而第 123 條第 1 項即係此所指對於資訊委員之要求，需注意者，該準則要求之範圍仍僅限定在 ISS 內。而對該準則，DPA 2018 第 123 條 2 項進一步地賦予資訊委員修訂之權，但仍須分別就兒童、家長、代表兒童權利者、兒童發展專家、貿易團體代表等不同面向，與國務卿諮詢（第 123 條第 3 項）。如資訊委員認為需修正，則在準備上的考量點必須至少包括：兒童在不同的年齡層有不同需求之事實，以及英國就聯合國兒童權利公約所應負擔之責任。

為此，ICO 提出適合年齡設計：線上服務實踐準則(Age appropriate design: a code of practice for online services)，[178]需注意者，因為時程關係，該準則尚未經英國議會審認，因此尚不具效力。在該準則中仍再次重申相關政策係基於聯合國兒童權利公約之要求，且此準則之出發點係應用符合比例且以風險為基礎(proportionate and risk-based)之考量方法。為此，對於兒童關於以下幾種基本權利與自由，應特別確認其保障：表現自由、思想、良心與宗教自由權、結社自由權、隱私權、藉由媒體而獲得資訊之權（並有適當保護以避免因來自資訊物質上之傷害）、適合其年齡之玩樂與參與互動活動之權、保護免受經濟、性或其他形式的剝削之權利。

該準則之規範列出了 15 種適合年齡的設計標準，反映了以風險為基礎的方法。重點是提供預設(default)的原始默認設置，以確保預設情況下兒童能夠最大程度地使用線上服務，同時最大程度地減少個資蒐集與利用。再者，這些設計標準的涵蓋範圍包括「推論資料(inferred data)」[179]，也就是根據其線上活動和通常基於內容消費的行為，而與他們相應配對的資料和特徵。需特別注意的是，因為該準則與線上通訊活動

[178] ICO, Age appropriate design: a code of practice for online services, https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/.
[179] Ibid., 22.

相關，亦涉及電子傳銷訊息，因此與隱私暨電子通訊規則(Privacy and Electronic Communications Regulations, PECR)亦有相關。

這 15 個設計標準分別是：

1. 兒童最佳利益[180]：在設計和開發可能會被兒童瀏覽或使用的線上服務時，應首先考慮兒童的最大利益。
2. 個資保護影響評估(DPIA)：進行 DPIA 評估和減輕由於資料控管者（即 ISS 提供者，下同）的個資處理而可能瀏覽或使用資料控管者服務的兒童的權利和自由的風險。此需考慮到不同的年齡、能力和發展需求，並確保資料控管者的 DPIA 遵循此規範進行建構。
3. 適合年齡的應用程序：採用以風險為基礎考量的方法來識別個別使用者的年齡，並確保資料控管者將此標準有效地應用於兒童使用者。年齡之確定可以適合資料控管者的資料處理所帶來的兒童權利和自由風險，或將此標準應用於所有使用者。
4. 透明度：資料控管者提供給使用者的隱私資訊以及其他已發布的條款、政策和社區標準均必須簡潔、醒目並且使用適合兒童年齡的清晰語言。在啟動使用時，還需提供有關資料控管者如何使用個人資料的「小篇幅」解釋(‘bite-sized’ explanations)。
5. 有害使用資料：資料控管者不得以已證明不利於其健康的方式使用兒童的個人資料，或違反行業行為準則，其他法規規定或政府建議的方式使用兒童的個人資料。
6. （個資保護）政策和社區標準：維護資料控管者自己發布的條款、政策和社區標準（包括但不限於隱私政策、年齡限制、行為規則和內容政策）。
7. 預設設置：預設情況下，設置必須為「高度隱私」（如要使用

[180] 聯合國兒童權利公約第 3 條：在與兒童有關的所有行動中，無論是由公共或私人社會福利機構、法院、行政機關或立法機構採取的，兒童的最佳利益都是首要考慮。

其他預設設置，除非資料控管者具有為兒童的最佳利益之正當化理由）。

8. 資料最小化：資料控管者僅蒐集和留存提供兒童積極而有意識地參與的服務選項所需要的最小數量的個人資料。並且，應讓兒童能選擇他們希望啟動的服務選項。
9. 資料共享：除非資料控管者出於充分考慮兒童的最佳利益，否則不得揭露兒童的資料。
10. 地理位置定位：預設情況下，關閉地理位置定位選項（除非資料控管者能說明一個令人信服的理由，即考慮到兒童的最佳利益而將地理位置預設開啟）。啟用位置追蹤時，應為兒童提供明顯的標示。在每次結束對話時，使其他人都能看到兒童定位位置的選項必須預設為「關閉」。
11. 家長控制：如果資料控管者提供家長控制，請給兒童適當的資訊。如果資料控管者的線上服務允許家長或照顧者監視兒童的線上活動或追蹤他們的位置，則在對其進行監視時，需給兒童一個明顯的信號。
12. 剖析：預設情況下，將使用剖析的選項設定為「關閉」（除非資料控管者能說明一個令人信服的理由，即考慮到兒童的最佳利益而將剖析之選項預設開啟）。僅當資料控管者採取適當的措施來保護兒童免受任何有害影響（尤其是提供有害於其健康或福祉的內容）時，才允許進行剖析。
13. 使用推力[181]技術(Nudge techniques)：勿使用推力技術來引導或鼓勵兒童提供不必要的個人資料，或關閉其隱私保護的設定。
14. 連結玩具和設備：如果提供之服務連結玩具或設備，需確保資料控管者提供有效的工具，以符合此準則。

[181] Nudge 這個概念出自 Richard H. Thaler & Cass R. Sunstein 所著作 Nudge: Improving Decisions About Health, Wealth, and Happiness 一書，書中知名例子即為荷蘭 Schiphol 機場的男廁小便斗裡頭貼有一隻蒼蠅圖案，竟然能有效降低男性「尿歪」的比例達高到 80%，意指設計者就像是「選擇的設計師」（choice architect）一般，能藉由情境打造與物質安排──就像建築師設計房屋一樣──可以促進使用者做出正確的決定與舉動。在此，則指政策或使用者控制選項之設定。

15. 線上工具：提供重要且易於使用的工具，以幫助兒童行使其個資保護權利和通報問題。

在這個實踐準則的最後兩個部分分別是對 ISS 提供者所需踐行之課責。該準則要求 ISS 提供者，也就是兒童之資料控管者應該實施一個課責計劃，以有效地解決此實踐準則中的標準。該計畫可以根據 ISS 提供者的規模和資源或其業務、組織以及線上服務中固有的兒童風險來量身定做。ISS 提供者應該不斷評估和修訂該計劃，並進行一些調整以反映兒童隱私環境的變化，並應該在任何內部或外部責任報告中，對照該準則中的標準進行報告，並引入有關兒童隱私的 KPI（關鍵績效指標）以適當地回應[182]。又，依據 GDPR 第 30 條第 1 項，各項個資處理紀錄應予以保存。

再者，關於 DPO，如果該 ISS 提供者已任命 DPO，則應由 DPO 來推動該準則；如果以這種方式組織業務，則應由董事會高級管理人員監督。對於可能沒有這種正式結構的小型企業，則需確保關鍵人員理解兒童的隱私，並被視為重要的企業優先事項，並瞭解該關鍵課責制措施仍然很重要[183]。

至於就 ICO 作為監管機關之執行面向來看，ICO 將根據適用法律並根據其「監管行動政策(Regulatory Action Policy)」採取適當措施，透過一系列主動審核來監控對該準則的遵守情況，以執行基本的個資保護標準[184]。而為了確保依照比例原則進行有效的監管，ICO 將以最重要的權力為目標，將重點放在涉嫌重複或故意不當行為或嚴重違反法律的組織和個人身上。

---

[182] ICO, Age appropriate design: a code of practice for online services, https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/, 87.

[183] Ibid.

[184] ICO, Regulatory Action Policy, https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.

另外就舉證言，如果 ISS 提供者不遵循此準則，則可能很難證明 ISS 提供者的個資處理是公平的並且符合 GDPR 或 PECR。而對於違反 GDPR 或 PECR，包括在處理兒童的個人資料時違反了相關法律規定的行為，ICO 有包括發出警告、譴責和罰鍰等各種職權。

七、 個資保護長

(一) ICO 與 DPO 之關係

由於 GDPR 應可解釋為較傾向期待會員國建立集中式之中央監管機關，並賦予其相當之獨立性保障，因此與我國目前的分散式監管策略下各中央目的事業主管機關與地方政府兼任個資監管機關不同，並無所謂地方監管機關。然則，依 GDPR 第 37 條第 1 項規定，符合下列三種情況之一之資料控管者，即應指派 DPO：(1)公務機關處理個資、(2)核心業務即為處理個資，且該處理個資行為需對當事人，並進行大規模的常態性及系統性監控、以及(3)核心業務為大規模的處理特種個資或刑案個資。

準此，身為會員國的英國在其中央各部會與地方政府機關等公務機關，即應依照 GDPR 第 37 條第 1 項第 1 款之規定設置 DPO，因此相對應地，DPA 2018 2018 在第 69 條以下規範有 DPO。在說明其設立與職權內涵之前，必須先釐清一個基礎前提：何以需在各機關設立 DPO？

(二) 設立 DPO 之理據：課責原則

學者對此認為 DPO 之設立係在體現課責原則(Accountability Principle)之要求：在 GDPR 第 5 條第 2 項中明文揭示資料控管者必須遵守前項之所有個資保護原則，包括合法公正與透明原則(lawfulness, fairness and transparency)、目的限制原則(purpose limitation)、資料最小化原則(data minimisation)、正確原則(accuracy)、以及整全與保密原則

(integrity and confidentiality)等[185]。那麼，我們必須進一步來追溯地問：又為何需要課責原則的具體化措施呢？究其原因，在於雖然個資保護在歐盟國家以資料保護指令(Directive 95/46/EC)的施行下已然推行多年，但是個資保護之觀念與具體的保護措施仍嫌薄弱且在各會員國之間存有落差，造成對資料控管者與政府就個資保護與資訊隱私言之缺乏信任與信心[186]。然而，該等當事人與控管者、受託處理者彼此之間缺乏信任之情狀，對於以資料為導向(data-driven)之科技、經濟甚至法律發展來說，都具有負面深遠影響[187]。爰此，課責原則必須真正地被具體實踐，不過為何設立 DPO 會是具體實現課責原則的手段之一呢？

論者認為，透過 DPO 之制度建立，不僅導入遵守各項個資保護基本原則之課責功能，更能使得該等基本原則更有效力(effective)，以及有效率(efficiency)地[188]被落實：與分散式兼管個資保護事項的傳統官僚行政制度不同，因為該等 DPO 有其專業且專責該等事項，因此能有效地運用其相配之資源與能力以達成其法律上保護當事人個資之責任，並且在該等個資保護責任與其他官僚庶務分立之情況下，有更大之機會避免利益衝突之發生。又，基於所有的公務機關均必須設有該職，則其覆蓋性更為全面，避免因為人力資源或預算微弱之偏遠行政機關發生個資事件時，無法處理而造成弱勢當事人受到權利侵害而難以有效救濟之問題。

再者，本報告亦認為尤其是公務機關 DPO 制度之建立，因為其理論上具有個資保護之專業能力，且在中央監管機關的統合與合作下，

[185] Peter Carey (2018), Data Protection: A Practical Guide to UK and EU Law, Fifth Edition, OUP, 224-226.
[186] Ana-Maria Brezniceanu, 'Data Protection Officer - a new profession in public administration?' (2017) 55 *Revista de Ştiinţe Politice* 80.
[187] Waldman AE, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge University Press 2018). Also, Ari Ezra Waldman, Privacy as Trust: Sharing Personal Information in a Networked World (March 1, 2014). 69 University of Miami Law Review 559 (2015).
[188] Ana-Maria Brezniceanu, 'Data Protection Officer - a new profession in public administration?' (2017) 55 *Revista de Ştiinţe Politice* 80.

較容易於各公務機關就個資保護之機構體系交互作用形成緊密連結之有機體，而不至於因為個資保護僅係其監管服務事務而臨事猶豫，推諉卸責。倘若以我國目前相關規範看來，或許以行政院消費者保護會及各地方政府消費者保護官之機構體系比擬，在一定的程度上，有其借鏡之處。

最後，因為 DPO 係常設職位，因此對於平時之包括個資教育宣導與定期稽核等職權功能，較能有效發揮，並能促進具有持續性特質之課責原則之實現。

就 ICO 對 DPO 之設立基礎相關說明看來，其亦明白地指出 DPO 能使得公務機關與企業等資料控管者展現出其對資料保護之遵循，並實現課責原則[189]。然而須注意者，ICO 認定就英國 DPA 2018 來看，課責原則之內涵實踐範圍包括接受與落實個資保護政策、採取個資保護之設計與預設(taking a 'data protection by design and default' approach)、個資相關契約義務之釐清、當事人保有個資處理活動之文件、採取適當的資安保護措施、蒐證與匯報個資事件、執行機關或企業個資風險評估、制定個資處理行為準則與授與相關認證，以及指定 DPO 等[190]，但是 DPO 在此並不是由其本身來承擔所有以上之功能，而是協助資料控管者與受託處理者來落實以上個資保護原則，並擔負重要之角色。換句話說，真正擔負起個資保護基本原則之落實與滿足責任者，乃是資料控管者或受託處理者。

(三) DPO 之設立與職權

就之所以 DPO 須設立之緣由分析後，接下來需面對之問題在於就

[189] ICO, Data protection officers, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/.

[190] ICO, Accountability and governance, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/.

DPO 之設立相關問題，包括其指定、遴選條件等，提出說明。

對於 DPO 的概念，大部分的閱讀者在乍聽之下通常誤會將其理解為係依據企業或團體人數之多寡而決定其是否須設置 DPO，然而事實上個資控管者是否須設立 DPO 之判斷標準，乃係依據其團體/組織所需主要處理個人資料行為，以達成該等團體之設立目的。而正因為政府機關無論為任何行政行為以達成其施政目的，均須透過處理個資（甚至是特種個資）為之，因此預設地要求政府機關必須設置 DPO。又，基於司法機關/法院之司法行為並非行政上行為，因此就其司法功能之部分，不需設立 DPO。需注意者，解釋上司法機關如為司法行政事項之行為，因為仍係踐行行政行為，仍須設置 DPO。因此在 DPA 2018 第 30 條第 1 項關於公務機關(competent authority)的定義，即 DPA 2018 附件 7 之內容，包括了法院與執法（檢、警）機關。換言之，事實上該等規範包含了所有的公務機關，均須設置 DPO。[191]

基於上述說明，在解釋上關於公務機關之定義範圍宜採取擴張解釋，將公務機關於個資保護事項指定 DPO 之範圍採最廣之解釋。其對於應設立 DPO 之公務機關解釋範圍，包括踐行司法行為的法院以外的各級公務機關，以及雖非公務機關但受委託行使公權力或公共服務者。

那麼英國 DPA 2018 對於個資法上的公務機關，又是如何認定？在此，基於個人資料保護在公務機關之面向上最相關，也最常競合者即屬政府資訊公開法之規範，因此 DPA 2018 在其第 7 條第 1 項第 a 款即明文規定將其定義指向 2000 年（政府）資訊公開法(Freedom of Information Act 2000, FOIA 2000)之定義[192]，而不為另外規範。而揆諸 FOIA 2000 第 3 條，則除前述公務機關範圍內，另包含公營事業

[191] See: Peter Carey (2018), Data Protection: A Practical Guide to UK and EU Law, Fifth Edition, OUP, 227.
[192] DPA 2018 第 7 條第 1 項第 b 款則是在蘇格蘭部分指向其政府資訊公開法。

(publicly-owned company)，這是因為公營事業事實上仍有相當大之可能性基於股份持有之指揮關係，而使公務機關保有之個資直接或間接流向該等事業[193]。須注意者，雖然在解釋上我國大法官釋字第 269 號解釋曾說明「依法設立之團體，如經政府機關就特定事項依法授與公權力者，以行使該公權力為行政處分之特定事件為限，有行政訴訟之被告當事人能力」，然就前述關於 DPO 之公務機關解釋應盡量為最廣義解釋，且是否具當事人適格與 DPO 似並無直接關聯，因此解釋上仍無妨將公營事業視為應設立 DPO 之公務機關。另外，如果同一資料控管者同時處理公務機關與非公務機關之持有個人資料，則僅就其處理公務機關持有個資部分，需指定 DPO[194]。

(四) DPO 之職權解釋與要求：與中央監理機關之連動

各公務機關之 DPO 職權，與中央專責監管機關即資訊委員之職權連動，合成英國個資保護監管的中央與地方機關之權限問題。而關於中央監管機關即資訊委員之權責，前已略述，則中央與地方監管機關權限問題下一階段之討論，即在確認各公務機關 DPO 之職權。其職權任務方面於 GDPR 之規定包括有落實所有相關個資保護規範、監理特殊之個資處理事件，例如個資保護影響評估、辦理教育宣導與教育訓練以提升組織人員之個資保護意識與水準，以及最重要者與中央個資監理機關就個資保護事項合作等。為了滿足前述職務任務需求，其聯絡之方式亦應公開，同時，也正是為了滿足履行該等職務之需求，因此相應之硬體環境設備與資源等，亦應相對應地提供予 DPO。並且，解釋上因為 DPO 落實以上所有職權均須透過對於該公務機關所持有之個資的接近使用，因此原則上應賦予其近用機關保有個資之權限。

就英國 DPA 2018 言，對於 DPO 之職權大致上與 GDPR 相同，並

[193] 須注意者，在 DPA 2018 中公務機關扣除了教區委員會(parish council)，其係英國之初級地方自治機關，但我國尚無類似建置。

[194] CIPL, Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation, November 2016, 14.

且在第 71 條第 1 項第 e 款中對於 DPO 監管該公務機關資料控管者以符合個資保護政策需求之規範上，明文例示包含對個資保護政策責任之分配、提升對個資保護政策之關懷、訓練處理個資過程經手之人員，以及對該等政策之監理與稽核等任務與責任。

關於對 DPO 的要求，則除表現在 GDPR 第 37 條第 5 項之專業品質以及能夠履行義務之能力等兩個法律上要求外，論者亦認為需有道德之要求。

先就對 DPO 之要求來看，第一個會碰到的問題或許必須要先問：GDPR 是否要求 DPO 須以自然人為限？就文義解釋言，基於諸如 GDPR 第 38 條第 2、3 項來看，分別有「his or her」、「he or she」之文字（代名詞），解釋上似乎著重於自然人之觀點，然而基於 GDPR 第 37 條第 6 項 DPO 除可以資料控管者或受託處理者之工作人員(staff member)為之外，亦可以基於服務契約而履行契約條款義務者，此時對後者之解釋，則似乎不限於自然人，法人亦得為之[195]。又，對比 DPA 2018，則第 69 條以下並無限制自然人之文字，因此本報告對此認為應不限於自然人方得擔任 DPO，法人亦得為之。

再就關於 DPO 專業能力與履行法定義務之要求言，觀諸 GDPR 第 39 條賦予的諸多法遵業務以及與中央監管機關的合作要求來看，似乎以法律專業技術人員較為適合從事該職務，但 DPO 之專業領域基於資料科技之日益進展與專業，仍應積極吸引跨領域人才如資訊科技、公共行政等領域，因此仍不應專以法律人才為限，但應鼓勵跨領域人才至少習得法律基礎專業為妥。

末就 DPO 之倫理要求言，大致上應與中央監管機關之成員要求相同，須具課責之要求以完成其職務。然而與中央監管機關的獨立性要

[195] CIPL, Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation, November 2016, 21.

求不同，DPO 係為公務機關內編制成員時，具有從屬性格；而外聘之 DPO 則基於契約履行以及對締約相對人之良善對待義務因此對於期待該等 DPO 具有高度之獨立性以監管個資保護事項，相較中央監管機關來說，道德要求較弱。然而，相較而言，公務機關內部成員而為 DPO 者，應較外部選聘之 DPO 熟悉該組織，因此理應擔負較高之資料治理與政策角色，而外部選聘之 DPO 於道德要求上仍應投入充分時間精力與資源，以滿足 DPO 之職責與契約上義務。最後，以英國 DPO 制度言，雖然賦予一定之獨立性以履行其任務，但相較於中央監管機關在預算、人事、編制以及職權之獨立性保障來說，仍有一定之機關從屬性格。因此，雖然對於 DPO 不會因為履行其義務而受罰，但是其對機關之保密要求與利益衝突揭露等原則，需特別注意。

最後必須加以釐清者，在分析完 DPO 之職權任務後，讀者或實務工作者經常誤會而認為 DPO 的所有職責都是在確保個資保護事項得到滿足，但事實上確保個資獲得保障的義務，乃係資料控管者或受託處理者之責任，而 DPO 在公務機關中，只是該等任務重要的核心協力者罷了[196]。

[196] ICO, Data protection officers, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/.

第三章　德國個人資料保護法制介析及落實 GDPR 之實務狀況

第一節　法制沿革

為保障個人權益不致因儲存、傳遞、更正及刪除等資料處理過程而受損，德國於 1977 年 1 月 27 日即制定「處理個人資料濫用防治法」（Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung），一般稱為「德國個人資料保護法」（Bundesdatenschutzgesetz，BDSG）（以下簡稱德國個資法），並行之有年。但隨著 90 年代後期資訊科技及網際網路的高度發展，個人資料以前所未見的規模，大量地被蒐集、彙整、分析，甚至與其他資料進行連結與比對，既有之個人資料保護規範，面對此一變遷，顯已不足因應，隨著眾所矚目之歐盟第 2016/679 規則（GDPR）以及歐盟 2016/680 指令（刑事司法中之個人資料保護指令），於 2016 年 4 月間問世，德國隨後亦於 2017 年 6 月 30 日公布新修訂的聯邦個資法，進行結構性之調整，由原先之 48 條大幅擴張為 85 條條文，並配合 GDPR，於 2018 年 5 月 25 日同步施行，接續於 2019 年 11 月 20 日公布施行對 GDPR 第二次調適之相關修法[197]，其中德國個資法益有相應之微幅調整。

有鑑於 GDPR 所規範者，係歐盟地區之個人資料保護法制框架，作為「規則」，其雖具備有直接拘束各會員國內國法制之效力，但 GDPR 立法過程中，仍不免面臨眾多利益衝突與政治角力，因此，GDPR 在指引出歐盟個人資料保護行進大方向的同時，仍透過置入各式「空白授權規範」，以「同中求異」之模式，讓各會員國之內國立法者，依據各國之實際情況再行規範。因此，GDPR 之具體實踐，若得透過觀察一個國家體制內，立法、行政以及司法權之交互作用，分析並探究其落實與執行 GDPR 規範之作法，對於時值個人資料保護制度轉型關鍵期之我國，當具實益。

[197] 關於該次修法所配合修正之法規，共計 155 部，請參考本報告附錄四「德國 2019 年 11 月 20 日因應 GDPR 第二次調適修正法規名稱」。

德國個人資料保護法制實以德國基本法（Grundgesetz）所保障之秘密通訊自由與資訊自決權（Grundrecht auf informationelle Selbstbestimmung）為中心開展，針對網際網路的崛起與相應科技設備之發展，更進一步透過德國聯邦憲法法院之判決，自一般人格權導出一新興之基本權類型：「保障資訊科技系統之秘密性與完整不可侵犯性之基本權（Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme）」，一般簡稱為「電腦基本權(Grundrecht auf Computerschutz)」，其保障範圍擴及使用所有資訊科技系統而產生、分析及儲存的所有資料，並不僅侷限於個別的網路通訊過程，就基本權主體因信任該系統之秘密性而交付資料，卻因系統遭第三人侵入或非法利用，致使資訊系統所承載之資訊、資料與應具備之功能受損，導致其完整性受到干預，將關注重心置於資訊系統使用過程不受干擾及該系統不被任意擷取之面向，區分其與資訊自決權之保障內涵，並予以特別保障[198]。

承接德國基本法對於基本權保障之誡命，德國立法者進而於法律位階尋求具體實踐：首先，制定德國個資法作為個人資料保護之基準法，提供處理個人資料一般性之法制框架；另，透過相關特別法之制定，以因應特定領域個人資料保護之需求，例如：電子媒體法（Telemediengesetz, TMG）、電信通訊法（Telekommunikationsgesetz，TKG）、社會法典（Sozialgesetzbuch，SGB）等，一方面達成將歐盟相關指令轉換為內國法規範之要求，另一方面，藉此提供人民不落科技發展之後的個人資料保護[199]。配合 GDPR 之制定與施行時程，德國個資法之法制架構亦調整為以下四個部分：

---

[198] 關於此一新興之「電腦基本權」之介紹與討論，Vgl. Jotzo,Florian, Der Schutz personenbezogener Daten in der Cloud, 2013, S.41-43.Wolff, Heinrich Amadeus/ Brink, Stefan, Datenschutz in Bund und Ländern, München: C.H. BecK, 2013, S. 88-89. 蔡宗珍，憲法人格權之保障及其界限-兼論網路人格權保護之憲法挑戰，第 9 屆憲法解釋之理論與實務學術研討會，中央研究院法律學研究所，2013 年 6 月 21、22 日，頁 21-23。

[199] Simits, Spiros(Hrsg.), Bundesdatenschutzgesetz, 8. Auflage, 2014, Einleitung S. 119-123. Tinnenfeld/Buchner/Petri, Einführung in das Datenschutzrecht, 5. Auflage, 2012, S.212-213.

第一部分，屬總則規範，針對共通性規定予以規範，包括適用範圍及定義（第 1、2 條），處理個資之合法要件（第 3、4 條），公務單位（öffentliche Stelle）[200]之 DPO（第 5-7 條），個人資料保護暨資訊自由監察官（第 8-16 條），EDPB 之代表及主要聯繫單位（zentrale Anlaufstelle）（第 17 條），聯邦及各邦監督機關就歐盟業務之管轄劃分與合作（第 18、19 條）以及救濟（第 20、21 條）。

第二部分，則係因應 GDPR 所為相應之規範，包括特種個人資料之處理及目的外之處理（第 22-25 條），特殊之處理情形（第 26-31 條），當事人之權利（第 32-37 條），資料控管者及受託處理者之責任（第 38、39 條），罰則（第 41-43 條）及救濟（第 44 條）。

第三部分，乃針對歐盟 2016/680 指令（刑事司法中之個人資料保護指令）為相應之規範，其規範內容包括適用範圍、定義及一般性原則（第 45-47 條），個人資料之處理（第 48-54 條），當事人之權利（第 55-61 條），資料控管者及受託處理者之責任（第 62-77 條），向第三國及國際組織為資料傳輸（第 78-81 條），監督機關之合作（第 82 條）以及責任與處罰（第 83、84 條）。

第四部分，則是針對歐盟第 2016/679 規則（GDPR）以及歐盟 2016/680 指令適用範圍外之處理個資行為，進行特別規定（第 85 條）。

第二節　德國個人資料保護之法制框架與特色

一、 監管機關之中央與地方權限

GDPR 就個人資料保護之監督，最終仍維持指令時代所建構之二

[200] 相較於 GDPR 以「資料控管者（Verantwortlicher）」作為其規範對象統稱之方式，德國個資法仍舊保留了其既有之「公務單位（öffentliche Stelle）」及「非公務單位（nicht öffentliche Stelle）」之規範模式，關於公務單位與非公務單位概念之界定，請參考德國個資法第 2 條。

根支柱（Zwei-Säulen-Modell）監管模式[201]。第一根支柱係藉由課予資料控管者及受託處理者設置個資保護長（Datenschutzbeauftragte）之義務；第二根支柱則是要求各會員國應建立一或多個監督機關，並強調監督機關應具備之獨立性。此與德國就個人資料保護採行之監管模式，本質上並無太大差異。針對 DPO，其雖非 GDPR 所稱監督機關，而屬要求資料控管者及受託處理者應自律採行之內控監管機制，但考量其功能與任務，皆與監督機關之職權密且相關，於個資保護之監管體系中，亦扮演相當關鍵之角色，故亦將其納入為簡要說明。以下將就德國個資法所建立之監管模式，分別說明。

(一) DPO 之設置

1. 公務單位之 DPO

在第一根支柱下，德國個資法亦要求應建立 DPO 之監管架構。針對公務單位，包括參與市場競爭之公營事業，德國個資法第 5 條均要求應設置 DPO，但可視其組織型態與規模，由多個公務單位任命共同之 DPO（德國個資法第 5 條）。德國個資法第 7 條特別強調 DPO 所擔負之任務，至少包括：

－針對負責處理個人資料之公務單位及其所屬人員，告知其依據本法或其他與個人資料保護相關法令，包括為轉化歐盟第 2016/680 號指令所發布之法令，所負有之義務並提供諮詢；

－監管本法或其他與個人資料保護相關法令之遵行，包括為轉化歐盟第 2016/680 號指令所發布之法令，以及公務單位對於個人資料保護所採行之策略，包括對於資料受託處理者之職務分配、敏感化、教育訓練，和與其相關之審查；

[201] Voßhoff, Andrea/ Hermerschmidt, Sven, Endlich! - Was bringt uns die Datenschutz-Grundverordnung, PinG 2/2016, S. 58.

－提供與個人資料保護影響評估相關之諮詢，並依據本法第 67 條監督其實施情形；

－與監督機關共同合作；

－就與處理個人資料相關之疑義，作為監督機關之對口單位，包括依據本法第 69 條所採行之事前協商以及針對其他問題所提供諮詢。

2. 非公務單位之 DPO

對於非公務單位部分，德國個資法第 38 條明定，具有 20 人以上專責自動化處理個人資料規模之非公務單位，應設置一名 DPO[202]。另外，針對依據 GDPR 第 35 條負有採行個資影響評估義務之控管者或受託處理者，或是其業務上基於（匿名）傳送個人資料之目的或進行市場或意見調查之目的而處理個人資料時，則不受前述受託處理者數之限制，均應即任命 DPO。

(二) 專責監督機關之設置

由於德國係採行聯邦體制，聯邦下共有 16 個邦，針對個人資料保護監督權責之劃分，於聯邦層次，依據德國個資法以及聯邦資訊自由法（Informationsfreiheitsgesetz，IFG）於聯邦層次建置「聯邦個人資料保護暨資訊自由監察官（Bundesbeauftragte für Datenschutz und Informationsfreiheit, BfDI）」，其所帶領之聯邦個人資料保護及資訊自由監察機構，作為最高聯邦機關之一，設於波恩（Bonn），另於柏林（Berlin）設有辦公室，其下目前配置約 180 名員額。依據德國個資法第 11 條之規定，聯邦個人資料保護暨資訊自由監察官係由聯邦政府提名，經聯邦議會（Bundestag）過半數同意後由聯邦總統任命，任期 5 年，得連

[202] 2019 年德國個資法修法時，將非公務單位處理個人資料之人數，由原先之 10 人提升為 20 人，適度放寬設置 DPO 之門檻，以減輕小型企業之負擔。

任 1 次，選任時應年滿 35 歲，並應特別關注其於個人資料保護領域之資格、經驗及專業知識，同時要求其應對於個人資料保護法制有充分之掌握且具備擔任法官或是更高等級行政職務之資格。

聯邦個人資料保護暨資訊自由監察官依據德國個資法與聯邦間屬公法上職務關係（öffentlich-rechtliches Amtsverhältnis）（德國個資法第 12 條第 1 項）。當聯邦個人資料保護暨資訊自由監察官行為有重大違失或無法達成履行任務所應具備之要件時，經聯邦議會主席之提議，由聯邦總統解除其職務（德國個資法第 12 條第 2 項第 2 句）。

獨立性向來是個人資料保護專責機關被強調之重點，德國藉由 2017 年之修法，將聯邦個人資料保護暨資訊自由監察官應具備之獨立性，明定於德國個資法第 10 條，賦予其履行任務及行使職權時，完全獨立（völlig unabhängig）之地位，其不受來自外部之直接或間接影響，亦無須請示或服從指令。並僅於不影響獨立性之範疇內，就經費稽核受聯邦審計部之監督。

於邦之層級，亦分別設有邦個人資料保護監察官（Landesbeauftragte für den Datenschutz ，LfD），各邦多於其個人資料保護法中，規範其設立、組織及職權[203]。歐洲法院曾於 2010 年 3 月 9 日作成之 C-158/07 判決中，認為德國未讓非公務單位之監督機關以「全然獨立」（in völlig Unabhängigkeit）之型態履行其任務，違反歐盟 95/46/EG 指令第 28 條第 1 項之規定，德國亦因此修法，明定個人資料保護暨資訊自由監察官依法獨立行使職權，力求排除行政干預，確保歐盟所要求之獨立性[204]。

---

[203] Kühling/Seidl/Sivridis, Datenschutzrecht, 3. Auflage, Heidelberg: C.F. Müller, 2015, S.231. 於部分邦之個人資料保護監察官，亦同時擔負促進資訊公開之任務。

[204] 李寧修，預防性通信資料存取之憲法界限-以歐盟儲備性資料存取指令（2006/24/EG）之發展為借鏡，興大法學，17 期，2015 年 5 月，頁 128-129。Kruse Julia, Der öffentlich-rechtliche Beauftragte, 2007, S. 207 ff. Dieter Zöllner, Der Datenschutzbeauftragte im Verfassungssystem, 1995, S. 21 ff., 167-170. Wohlgemuth/Gerloff, Datenschutz, 3. Aufl., 2005, S. 143-145.

聯邦與各邦之個人資料保護監管權限，得細部劃分如下：

1. 聯邦個人資料保護暨資訊自由監察官（BfDI）

聯邦個人資料保護暨資訊自由監察官專責聯邦所屬公務單位之個人資料保護監管，並提供相關機構於個人資料保護與資訊公開事務之諮詢。其管轄及於聯邦所屬機關或其他聯邦公法機構，同時包括參與市場競爭之公營事業，例如：德國電信（Deutsche Telekom）處理個人資料之行為，即屬聯邦個人資料保護暨資訊自由監察官之管轄[205]。另外，針對由聯邦之持股佔多數或掌握多數決策權，且其委託人係屬聯邦公務單位之資料受託處理者（Auftragsverarbeiter），依據德國個資法第 9 條第 1 項第 2 句，亦將其視為公務單位，列屬管轄範疇。屬聯邦管轄者，例如：提供社會給付之德國退休保險聯盟（Deutscher Rentenversicherung Bund）、礦工工會（Knappschaft）或提供全聯邦疾病保險之機構，如 Barmer、DAK、TK 等；以及依據社會法典第二部所設置之公共機構，即就業中心（Jobcenter）…等。但就聯邦法院基於司法職權所為之個人資料處理行為，則非屬聯邦個人資料保護暨資訊自由監察官管轄之範圍（德國個資法第 9 條第 2 項）。

非公務單位原則上應屬各邦個人資料保護監察官之管轄範圍，但針對提供電子通訊服務、郵務服務（Telekommunikation- und Postdienstleistungen）或屬安全檢核法（Sicherheitsüberprüfungsgesetz）所納管之私人公司[206]，則例外地交由聯邦負責管轄。

2. 各邦個人資料保護監察官（LfD）

依據 GDPR 第 51 條第 1 項連結德國個資法第 40 條第 1 項之規定，各邦個人資料保護監察官主責監督非公務單位之個人資料處理行為，

[205] Schantz/Wolff, Das neue Datenschutzrecht, 2017, S.329.
[206] 依據安全檢核法第 1 條，該法所適用之對象，及於被相關機關交付或即將交付安全機敏任務或機密文件之人。

因此，私法領域中，例如公司、協會、團體或獨立營業者（如；醫師、稅務諮詢師）...等涉及處理個人資料之行為，皆屬其權限之範圍。而針對外國公司處理個人資料之行為，若該外國公司之母公司係設立於其他歐盟會員國，但亦於德國設有事務所，則交由該事務所所在地所屬邦為管轄；然而，當該外國公司於德國未設有事務所，或是該外國公司並未設於歐盟任一會員國，但以德國作為交易市場地點時，原則上依其行為地，由各邦為監管。若遇有爭議，而當事人欲提出異議時，則得就近向其居所所在地之邦個人資料保護監察官提出。

另，其管轄範圍亦涵蓋各邦、各鄉鎮所屬機關或行政單位，例如：城鎮之行政單位、教育機關、青年局處、一般地方性之疾病保險機構...等。

3. 特殊領域之監管

由於 GDPR 第 51 條對於監督機關之設置，並未限制其數量，且針對特定領域，允許各會員國得就 GDPR 所預設之監管機制，包括 GDPR 第四章中關於 DPO 以及第六章之監督機關，為排除或例外規定，例如：GDPR 第 91 條第 2 項針對教會及宗教團體或機構以及 GDPR 第 85 條第 2 項就媒體之監管[207]。因此，德國於特定領域之個人資料保護監管，即有另外設置監察官之情形，例如廣電機構部分交由廣電個人資料保護監察官（Rundfunkbeauftragte für Datenschutz），或是教會個人資料保護監察官（kirchliche Datenschutzbeauftragte）[208]。以巴登-符騰堡邦（Baden-Württemberg）為例，該邦除設有邦個人資料保護監察官外，另依據其邦個人資料保護法第 27 條設置有廣電個人資料保護監察官，並依據教會個人資料保護法設有二位教會個人資料保護監察官（一位

[207] Schantz/Wolff, Das neue Datenschutzrecht, 2017, S.328.

[208] 針對教會之個人資料保護，另有適用於基督教教會之教會個人資料保護法（Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland，EKD-Datenschutzgesetz），以及適用於天主教教會之教會個人資料保護法（Gesetz über den Kirchlichen Datenschutz，KDG），分別於其中之第六章均規定建立對於教會個人資料之監督機制，即任命教會個人資料保護監察官，並明定其地位、職權、任務等相關規範。

天主教；一位基督教），共同作為邦層級之監督機關。由於德國不論是聯邦或邦層級之監督機關，均屬採行首長制之機關，故可能係考量領域之特殊性及其專業智識（Fachkunde）之要求，同時依據處理資料之數量、種類及其對於人民權利影響之程度，進行適度專業分工。

二、 個人資料特定目的外利用之要件

基於目的拘束（Zweckbindung）原則，個人資料必須基於確定、清楚且合法之目的為蒐集，且不應允許藉由與該目的不一致之方式進行處理（GDPR 第 5 條第 1 項第 b 款），由此可知，GDPR 要求原始蒐集目的與後續處理之目的間，應具有一致性（Zweckvereinbarkeit），一旦二者間具有一致性，即未違反目的拘束原則[209]；然而，一旦二者間無法取得一致性，此種目的外之處理原則上即非屬合法，但若符合 GDPR 第 6 條第 4 項明定之目的外處理要件，則仍屬合法，例如：取得當事人之同意或是得援引歐盟或其會員國之相關法律作為處理依據。針對後者，德國個資法第 23 條及第 24 條，即是於此種目的不具一致性之情形下，得例外合法處理個人資料之法律依據，並應同時符合 GDPR 第 6 條第 4 項所定「提供民主社會中所必要並合乎比例之措施，保護 GDPR 第 23 條第 1 項中所列目的」之要件。

因應大數據時代下資料再利用的高度需求，不論是 GDPR 或是德國個資法，對於個人資料特定目的外利用之要件，均適度放寬其要件，但亦同時要求應採行技術上或組織上之相應措施，以強化當事人權利保護。另外，GDPR 第 13 條第 3 項（直接向當事人蒐集個資之情形）及第 14 條第 4 項（間接向當事人蒐集個資之情形）中課以控管者（Verantwortliche）之告知義務，於此亦應予以關注，藉以確保當事人對於變更後之目的以及 GDPR 第 13 條第 2 項及第 14 條第 2 項之相關資訊，得有充分知悉與掌握之可能性。而基於檔案、研究或統計之目的而為處理之情形，依據 GDPR 第 5 條第 1 項第 b 款，未被視為目的

[209] Kühling/Buchner, DS-GVO, BDSG Kommentar, 2. Auflage, 2018, S.1378-1371.

外處理，並於 GDPR 中列屬於特殊處理之情形。

以下將德國個資法就一般個人資料及特種個人資料所定目的外利用要件，分予說明：

(一) 一般個人資料之目的外處理要件

德國個資法針對一般個人資料之目的外處理，分別規定於德國個資法第 23 條第 1 項（公務單位之目的外處理）及第 24 條第 1 項（非公務單位之目的外處理）中。公務單位若欲將個人資料於蒐集目的外為處理，與目的內處理相同，仍應限於履行職務之範圍內，且必須同時符合德國個資法第 23 條第 1 項所定情形之一。

1. 公務單位目的外處理一般個人資料

德國個資法第 23 條第 1 項下共 6 款，針對公務單位目的外處理個人資料之要件為規範：

－係為維護當事人法益，且無理由認為當事人會拒絕同意，且前述情形應屬明顯（德國個資法第 23 條第 1 項第 1 款）[210]；

－因對於當事人陳述之正確性有事實上之懷疑，而必須予以審核（德國個資法第 23 條第 1 項第 2 款），但若以此為由，廣泛地預先蒐集個人資料，則恐有倒果為因之謬誤，另外，本款之適用應限於未有其他侵害較小的手段足以達成目的之情形，例如直接向當事人進行查證。若單就本款文義，恐怕無法直接確認（與原始蒐集目的不同之）處理目的究竟為何，故其是否得符合 GDPR 第 23 條

[210] 但亦有主張以目的一致性進行檢視，當事人因獲益或免除不利益，而必然會提供同意之情形，應可認其變更後之目的與蒐集之原始目的間，並未存有不一致之情形，並未違反目的拘束原則，得直接以德國個資法第 3 條為據，而其列屬德國個資法第 23 條第 1 項第 a 款之目的外處理要件，雖非牴觸 GDPR，但並無規範功能。Kühling/Buchner, DS-GVO, BDSG Kommentar, 2. Auflage, 2018, S.1373.

第 1 項下任何一款，仍須依據個案為判斷[211]。

－為防止對公共利益之重大損害或對公共安全、軍事防衛或國家安全之危害，或為維護公眾之重大利益或確保稅務及海關收益，且屬必要（德國個資法第 23 條第 1 項第 3 款）[212]。本款主要係基於維護公益之目的為目的外處理，其運用為數不少的不確定法律概念，包括「公共利益」、「公共安全」、「國家安全」、「公眾利益」等，並透過「重大」適度限縮其範圍，而重大與否之判斷，應就該等公益與當事人法益妥適衡酌。前述不確定法律概念作為（目的外)處理之目的,仍有待立法者進一步立法,將其內涵具體化[213]，例如：對於公共安全危害之認定，即應配合警察法相關規定為判斷。其中「確保稅務及海關收益」，因與國家財政利益密切相關，亦一併納入。本款涉及變更後之目的，大致與 GDPR 第 23 條第 1 項第 a、b、c、e 款所定目的相當。

－為追訴犯罪或追究違反秩序之行為，為強制執行或執行刑法第 11 條第 1 項第 8 款所定刑罰或措施、少年法院法所定感化教育或教養方法、或為強制執行罰金，且屬必要（德國個資法第 23 條第 1 項第 4 款）[214]，本款涉及違反刑事法及秩序法之行為，且限於必要之情形，亦即該目的已然無法藉由其他方法加以達成時，方屬之。本款涉及之變更後目的，與 GDPR 第 23 條第 1 項第 d 款所定目的相當。

－為防止對他人權利之嚴重損害所必要（德國個資法第 23 條第 1 項第 5 款）[215]。其係以保護私人權益為目的，與 GDPR 第 23 條第 1 項第 i 款所定目的相符，私人不限於自然人，法人亦可當之。權利

[211] Kühling/Buchner, DS-GVO, BDSG Kommentar, 2. Auflage, 2018, S.1373.
[212] 舊德國個資法第 14 條第 2 項第 6 款參照。
[213] GDPR 第 23 條第 1 項第 a 款參照。Kühling/Buchner, DS-GVO, BDSG Kommentar, 2. Auflage, 2018, S.1374.
[214] 舊德國個資法第 14 條第 2 項第 7 款參照。
[215] 舊德國個資法第 14 條第 2 項第 8 款參照。

類型如生命、身體、財產等均屬之，但損害應限於「嚴重」之情形。

－為履行監督及管理之職權，審計查核或執行對控管者之組織調查；此亦適用於基於教育及考試之目的透過控管者而為處理之情形，但須與當事人應受保護之法益未有衝突之範圍內為之（德國個資法第 23 條第 1 項第 6 款）。公務單位執行職務，往往需要運用監督及管制之手段作為輔助，然由於此二者間具備緊密之聯結關係，應可認為職務之履行屬主要目的，而監管則為從屬目的（Sekundärzweck），而前者作為原始蒐集目的，其與後者之變更後的處理目的，是否不具有一致性，而當然屬目的外處理之情形，恐不無疑義[216]。

2. 非公務單位目的外處理一般個人資料

德國個資法第 24 條第 1 項針對非公務單位將個人資料於蒐集目的外為處理之要件為規範，其合法要件包括以下二種情形，且均以相較於該目的外處理，當事人未有更值得保護之法益，作為其前提：

－須為防止對國家或公共安全之危害或為追訴犯罪所必要（德國個資法第 24 條第 1 項第 1 款），此一要件實與前述德國個資法第 23 條第 1 項第 3、4 款所定公務單位目的外處理要件相當相似，其所包含目的外處理之目的，分別得見於 GDPR 第 23 條第 1 項第 a、c、d 款中。然而，如前所述，於判斷該等不確定法律概念時，仍應配合其他相關法令為理解，例如對於防止公共安全之危害，其應輔以警察法相關規定為認定；而本款所稱「犯罪」，則應限於違反刑事法律之行為；另，由於安全之維護常另定特別法為規範，如刑事訴訟法第 161 條，依據德國個資法第 1 條第 2 項，特別規定得

[216] 同一要件得見於舊德國個資法第 14 條第 3 項，但其並未被列屬目的外處理之要件，而被視為屬於原始蒐集目的內所應涵蓋之範圍。Kühling/Buchner, DS-GVO, BDSG Kommentar, 2. Auflage, 2018, S.1375-1376.

優先適用，故適用德國個資法第 24 條第 1 項第 1 款之情況，即是如與執行維安或保全之私人公司，透過激進組織嫌疑名單過濾其工作成員[217]。

－係屬為適用、主張民法上請求權或為對抗民法上請求權所必要者（第 24 條第 1 項第 2 款），此一目的亦得見於 GDPR 第 23 條第 1 項第 j 款中，該民法上請求權之主張，不以已進入司法程序者為限。

(二) 特種個人資料之目的外利用要件

針對特種個人資料之處理，GDPR 之基本立場，乃原則不得處理，僅於符合法定要件時，方例外得予處理，並於 GDPR 第 9 條第 2 項明定例外之情形，但其中仍有給予各會員國極大發揮的空間，例如：

－該處理為資料控管者或當事人主張其基於勞動法或社會安全或保護之法令所享有之權利所必要（GDPR 第 9 條第 2 項第 b 款）。

－該處理係依據歐盟法或會員國法令，與其所欲達成目的間具合理關聯性（in angemessenem Verhältnis），維護個人資料保護權利之本質，並訂有保護當事人基本權利及利益之適當特殊措施，而基於有重大之公益理由，認有必要者（GDPR 第 9 條第 2 項第 g 款）。

－該處理係出於健康照護或為判斷受雇者工作能力之勞動醫學，為了醫學上之診斷、健康或社會領域之照護或治療或為了健康或社會領域之體系或服務之管理，依據歐盟法、會員國之法令或與擔任健康相關職業之成員（einem Angehörigen eines Gesundheitsberufs）間簽訂之契約，並符合第 3 項所定要件及保障，而認有必要者（GDPR 第 9 條第 2 項第 h 款）。

[217] Kühling/Buchner, DS-GVO, BDSG Kommentar, 2. Auflage, 2018, S.1378-1379.

－該處理係於公共衛生領域基於公益理由，例如為防範跨境之嚴重健康危害或為維護健康照護及醫藥產品的高品質及安全標準，並已依歐盟法或會員國法令採行維護當事人權利及自由之適當特殊措施，而認有必要者（GDPR 第 9 條第 2 項第 i 款）。

－該處理係依據歐盟法或會員國法令，與其所欲達成目的間具合理關聯性，維護個人資料保護權利之本質，並訂有保護當事人基本權利及利益之適當特殊措施，而依據第 89 條第 1 項基於公益之檔案儲存目的、學術或歷史研究目的以及統計目的，認有必要者（GDPR 第 9 條第 2 項第 j 款）。

於前述例外情形中，均留給各會員國之內國立法者，透過制定法律，創設特種個人資料例外處理之空間。另外，針對涉及基因、生物特徵或健康資料之處理，GDPR 第 9 條第 4 項亦允許各會員國維持或再另行訂定附加之要件。

相較於 GDPR 第 9 條對於特種個人資料所採「原則禁止，例外許可」之處理模式，德國個資法針對特種個人資料之規範架構，則係於德國個資法第 22 條中明定公務與非公務單位處理特種個人資料之要件（第 1 項），並輔以相應程序、技術之採行，以確保當事人權利之維護（第 2 項）。德國個資法對於開啟特種個人資料目的外處理之情形，則係分別規定於德國個資法第 23 條第 2 項（公務單位之目的外處理）及第 24 條第 2 項（非公務單位之目的外處理）中。

特種個人資料之目的外利用，應符合以下要件：

－一般個人資料目的外利用之要件，即分別規定於德國個資法第 23 條第 1 項（公務單位之目的外處理）及第 24 條第 1 項（非公務單位之目的外處理）中之要件；以及

－具備 GDPR 第 9 條第 2 項之例外要件或德國個資法第 22 條所定之

要件。

由前述可知，德國個資法第 22 條所定之要件，應屬德國個資法就特種個人資料之目的外處理，依據 GDPR 之授權，進一步制定之規範。德國個資法第 22 條第 1 項第 1 款，排除 GDPR 第 9 條第 1 項，就特種個人資料透過公務及非公務單位之處理，當其符合以下情形之一者，係屬合法：

－為行使自社會安全權利及社會保護所衍生之權利並承擔因此產生之相關義務，且屬必要者（德國個資法第 22 條第 1 項第 1 款第 a 目），其係呼應 GDPR 第 9 條第 2 項第 b 款之規定，德國就與基於社會權而生之個人資料處理情況，多係另行規範於社會法典中，其作為處理個人資料之特別法，得優先於德國個資法而適用。

－基於健康照護之目的、為判斷勞動者之工作能力、為醫學上之診斷、健康或社會領域之照護或處置、為健康或社會領域系統及服務之管理或基於當事人與健康職業成員之合約，並屬必要，且該個人資料係由醫護人員或具有相應保密義務之人員為處理，或於其監督下為處理（德國個資法第 22 條第 1 項第 1 款第 b 目）[218]。

－基於公共健康領域中公共利益之理由，如防護受到重大跨境之健康危害或維護較高品質及安全標準之健康照護、藥品及醫藥器材，且屬必要；於此須特別關注職業上及刑法上保密義務之遵守（德國個資法第 22 條第 1 項第 1 款第 c 目）[219]。

－基於重大公共法益而有急迫必要（德國個資法第 22 條第 1 項第 1 款第 d 目）；依據立法理由之說明，依據此目的所為之特種個人資料處理，即可能指向具有高度敏感性之得明確辨識特定當事人之

[218] GDPR 第 9 條第 2 項第 h 款參照。
[219] GDPR 第 9 條第 2 項第 i 款參照。

生物資料[220]。

透過公務單位處理特種個人資料之要件，德國個資法第 22 條第 1 項第 2 款嘗試將 GDPR 第 9 條第 2 項第 g 款所稱「重大公共法益」具體化，開啟與其密切相關之處理可能性：

－為防止對公共安全之重大危險所必要（德國個資法第 22 條第 1 項第 2 款第 a 目），於此就「公共安全」之認定，大多與警察法有密切之關聯，於此除要求危險須屬重大（erheblich）外，其涉及法益亦應以生命、身體、健康等重要法益為關注重心[221]。

－為防止對於公共利益之重大不利益或為維護公共利益之重大利益而有急迫必要者（德國個資法第 22 條第 1 項第 2 款第 b 目）；

－基於軍事防禦或為履行聯邦公法單位之跨國家或國際間義務之理由，於危機處理、衝突預防或人道措施之領域有其必要（德國個資法第 22 條第 1 項第 2 款第 c 目）。

前述要件於適用上仍留有相當之判斷餘地，例如「急迫必要」之認定，若僅單純援引德國個資法第 22 條第 1 項第 2 款下各目作為處理特種個資之依據，並不足夠，其同時必須釋明於個案中具體之公共利益究竟所指為何；其次，其明定利益權衡之義務，惟有當權衡控管者於處理所欲維護之法益與當事人因此所受損害之法益後，於前者為重之情形，方得為之；另，處理與其所欲達成之目的間，應合於比例，並應維護個人資料保護權利之核心內涵[222]。

然而，德國個資法第 22 條第 1 項作為填補 GDPR 第 9 條第 2 項所

[220] 此一要件原先僅屬德國個資法第 22 條第 1 項第 2 款所定公務單位處理特種個資之要件之一，於 2019 年 11 月 20 日修法時，將其移列同條項第 1 款，因此開啟除了公務單位外，非公務單位亦可據其處理特種個資。BR-Drs. 110/17，S.94.

[221] Kühling/Buchner, DS-GVO, BDSG Kommentar, 2. Auflage, 2018, S.1364.

[222] BR-Drs. 110/17，S.93.

定例外處理特種個人資料要件中之「內國法規範」，卻也招致以下批評：要件中大量承繼GDPR既有之文句，包括不確定法律概念及概括條款，對於相關規範之具體化並未有進一步之幫助，另外，亦可能有違反法律明確性原則要求之疑慮[223]。而於特殊處理情形中，德國個資法亦廣開對於特種個資利用之可能性，例如德國個資法第 26 條第 3、4 項（就業關係），第 27 條第 1 項（研究與統計）及第 28 條第 1 項（基於公益之檔案儲存），並同時限縮當事人權利所得主張之範圍[224]。

而德國對於健康資料之處理，尚未定有專法，但其規範係散見於聯邦及各邦之法律中，例如：德國個資法第 27 條對於基於研究或統計目的處理個人資料之規定；德國社會法典對於社會資料（社會法典第十部，第 67a 條至第 85a 條）、法定醫療保險（社會法典第五部，第 284 條至第 305b 條)及法定照護保險相關資料之處理(社會法典第十一部，第 93 條至第 111 條)；傳染病保護法第 9 條、器官移植法（第 13 條至第 15 條)、醫療器材法第 20 條第 1 項第 2 款等，均為適例。另外，聯邦經濟及能源部（Bundesministerium für Wirtschaft und Energie）亦針對非公務單位處理健康資料，創造經濟價值，就其適法性及應有之配套機制，提供相關指導[225]。

三、 去識別化之要件、程序、認定方式等規定

為使個人資料得以合法、適度地流通，去識別化技術之導入，即有其重要性。德國個資法一直以來，都將去識別化技術視為在維護當事人法益之適當且特定之措施中，所不可或缺者，但此次修正將原先於舊法中有定義之「假名化(Pseudonymisierung)」刪除，直接適用 GDPR 之規範。GDPR 第 4 條第 5 款將「假名化」定義為：「在不使用額外資

223 Kühling/Buchner, DS-GVO, BDSG Kommentar, 2. Auflage, 2018, S.1361-1362.
224 此部分請見：四、特殊處理情形之說明。
225 Bundesministerium für Wirtschaft und Energie, Orientierungshilfe zum Gesundheitsdatenschutz, 2018, https://www.bmwi.de/Redaktion/DE/Downloads/M-O/orientierungshilfe-gesundheitsdatenschutz.pdf?__blob=publicationFile&v=169（最後瀏覽日：2020/05/05）

料的情形下，無法將個人資料歸屬於特定個人的資料處理或利用方式；但該額外資料必須分別保管，並採取技術及組織上的措施，以避免個人資料被歸屬於一個已識別或足資識別的自然人」；另外，若得將個人資料轉化為「與已識別或足資識別的自然人無關的資訊」或「原本屬於個人資料，但經過去識別化處理，已無法（再）識別當事人」之資料，其因屬匿名之資料（anonyme Informationen）」，與個人資料之定義不符，自不受 GDPR 之拘束，而得放寬其處理之標準[226]。GDPR 及德國個資法，皆可見以上述「匿名化」及「假名化」之機制，作為適度鬆綁對於處理個人資料限制之配套[227]。

假名化之技術被使用於個人資料之處理過程中，降低特定人被識別之風險，但針對不同之資料、要件下處理之方式，恐怕所要求採行之安全維護措施，仍有其程度不同之差異[228]。德國個資法第 22 條第 2 項針對特種個資之處理，要求必須輔以相應程序、技術之採行，以確保當事人權利之維護；另外，對於特種個資之目的外處理，德國個資法亦以具備 GDPR 第 9 條第 2 項之例外要件或德國個資法第 22 條所定之要件為前提，因此，對於特種個人資料之處理，德國個資法第 22 條第 2 項所要求採行之「適當特定措施」，即與 GDPR 所要求之「適當技術及組織上措施」有異曲同工之妙，亦屬處理特種個人資料所不可或缺之要件，有其重要性。

德國個資法第 22 條第 2 項對於「適當特定措施」之擇定，實呼應 GDPR 第 9 條第 2 項第 b 款、第 g 款及第 i 款中「提供當事人之權利及

---

[226] GDPR 立法前言第 26 點參照。

[227] GDPR 所要求之適當安全措施，包括運用不可回復之去識別化資料或去連結資料，且應以前者為優先，似有鼓勵使用不可回復的去識別資料之意。Roßnagel, Europäische Datenschutz-Grundverordnung, 2017, S.234-237. Schantz/Wolff, Das neue Datenschutzrecht, 2017, S.408-413.

[228] GDPR 第 25 條第 1 項針對控管者及受託處理者為維護當事人權利，而應採行之適當技術及組織上措施，即要求其於擇定前述措施時，應同時將現行技術、執行成本及處理之性質、範圍、內容及目的，以及處理對當事人之權利及自由所生諸多可能且嚴重之風險等因素，納入考量。

法益適當保障」之要求，然而，針對資料控管者或受託處理者所採行之措施是否適當，其要求應同步關注技術之發展情形；採行之成本；處理之形式、範圍、狀態及目的；以及因處理而對當事人自由權利所招致風險發生之各種可能性與嚴重性。

德國個資法第 22 條第 2 項下有 10 款，其所定「適當特定措施」可能包括：

－採行技術及組織上之措施，以確保依據 GDPR 而為之處理得以完成（德國個資法第 22 條第 2 項第 1 款）；其與 GDPR 第 32 條及第 25 條之適用有密切關聯[229]。

－確保事後審查及確認個人資料是否以及由何人交付、變更或移除之措施（德國個資法第 22 條第 2 項第 2 款）：藉以強化個人資料處理歷程之透明性及可回溯性，與 GDPR 中亦常見之例如：歷程記錄（GDPR 第 30 條）或處理措施之記錄（GDPR 第 5 條第 2 項）等，有異曲同工之妙。針對特種個人資料，其應對其處理歷程進行全程記錄，而該記錄之保存期限必須事前透過風險評估確認並確實落實，在實務上可能因個人資料之性質而允許有異，特種個人資料之歷程記錄至少應保存 1 年；以數位形式保存之醫療記錄則是 10 年至 30 年間不等[230]。

－處理過程中參與者之敏感化（德國個資法第 22 條第 2 項第 3 款）。其係藉由組織上運作，課予資料控管者及受託處理者指導參與處理個人資料相關人員之義務[231]，此一任務多交由其內部 DPO 執行[232]，確保各該人員，對於其所擔負之義務，應充分知悉掌握並提供所需諮詢，亦得藉由辦理個人資料保護教育訓練，建立其對於

[229] Kühling/Buchner, DS-GVO, BDSG Kommentar, 2. Auflage, 2018, S.1366.
[230] Kühling/Buchner, DS-GVO, BDSG Kommentar, 2. Auflage, 2018, S.1366.
[231] 類似規定得見於 GDPR 第 32 條第 4 項之規定中。
[232] 請參考 GDPR 第 39 條第 1 項第 a 款。

合法處理個人資料應具備之知識與警覺，但資料控管者或受託處理者亦負有協力義務，提供其必要之協助[233]。然而，若僅是單純發放書面說明予以指導，而未配合經常性之考核與提示，對於特種個人資料之處理而言，即恐有未足[234]。

－任命 DPO（德國個資法第 22 條第 2 項第 4 款）；德國個資法第 38 條對於任命 DPO 之義務有所規範，但不同之處在於，德國個資法第 22 條第 2 項對於處理特種個人資料之情形下任命 DPO 之要求，無關乎其所屬人員數額、處理特種個人資料所致風險以及是否負有採行個人資料結果評估義務，皆負有任命義務[235]。

－將近用個人資料之範圍限於資料控管者及受託處理者之所在地內（德國個資法第 22 條第 2 項第 5 款）。此係沿襲於舊德國個資法中可見之「近用管制（Zugangskontrolle）」義務，以確保未享有權限者，不得處理個人資料，其限制包括地域之劃定，即「進入管制（Zutrittkontrolle）」，對於得以接觸個人資料處理系統之人員，透過如設定使用者帳戶密碼、晶片卡、生物特徵或加密等方式驗證其身分，確保未逾越權限[236]。

－將個人資料假名化（德國個資法第 22 條第 2 項第 6 款）。德國個資法中對「假名化」並未有定義性規定，而回到 GDPR 為適用。何時會有將個人資料假名化之義務，與個資保護影響評估之結果往往有極為密切之關係，例如針對醫院資訊系統，假名化即屬義務[237]。

－將個人資料加密（德國個資法第 22 條第 2 項第 7 款）。所謂加密，

[233] Kühling/Buchner, DS-GVO, BDSG Kommentar, 2. Auflage, 2018, S.1366.
[234] Eßer/Kramer/v. Lewinski(Hrsg.), DSGVO BDSG Kommentar, 6. Auflage, 2018, S.1485.
[235] Eßer/Kramer/v. Lewinski(Hrsg.), DSGVO BDSG Kommentar, 6. Auflage, 2018, S.1486-1487.
[236] Eßer/Kramer/v. Lewinski(Hrsg.), DSGVO BDSG Kommentar, 6. Auflage, 2018, S.1486.
[237] Kühling/Buchner, DS-GVO, BDSG Kommentar, 2. Auflage, 2018, S.1367.

係透過改變資料數列，使第三人無法辨讀其內容，而若欲回復，則必須透過特定數學演算式方得達成。特種個人資料及以數位型態儲存之個人資料，加密應屬合法處理之要件，尤其是潛在高度濫用風險之健康資料，若欲處理，則加密應屬最基本之要求[238]。若欲排除加密之限制，則須於依據 GDPR 第 35 條作成之個資保護影響評估中，特別註明其理由。

－確保與處理個人資料有關之系統及服務之能力、可信度、完整性、可用性與持久性，包括其在物理上或技術上突發狀況下迅速回復之能力、可用性及取得（德國個資法第 22 條第 2 項第 8 款），其目的在於確保個人資料之可用性。

－為維護處理之安全性，就技術性及組織性措施之有效性，建立經常性之查核、評估及評等之程序（德國個資法第 22 條第 2 項第 9 款），此一確保處理個人資料安全性之措施，應可望透過建立完善之內部及外部監管機制達成。

－確保就目的外之處理或傳輸訂定之特殊程序規範，符合德國個資法以及 GDPR 要求（德國個資法第 22 條第 2 項第 10 款）。其對於目的外處理以及向第三人為傳輸之情形，要求應建立特殊程序規範以供依循，此一程序性規範，與同條項第 9 款所稱「建立經常性查核、評估及評等技術性及組織性措施有效性之程序」，實有相當密切之關聯，另，GDPR 第 6 條第 4 項對於處理個人資料之合法要件中，對於目的外處理應關注之面向，於此亦應納入考量，另外，舊德國個資法中曾規定之紀錄以及對於處理目的之提示與經常性之查核與評估，皆為適例。

應注意者為，德國個資法第 22 條第 2 項所列出之 10 款適當特定措施，應屬例示規定而非列舉，其並未包含所有可能用於保護處理個

[238] Eßer/Kramer/v. Lewinski(Hrsg.), DSGVO BDSG Kommentar, 6. Auflage, 2018, S.1486.

人資料安全以及維護當事人權利之技術上、組織上措施，例如德國個資法第 27 條第 3 項針對基於科學或歷史研究目的以及統計目的處理特種個人資料，即有匿名化（zu anonymisieren）之要求，而於匿名化前，亦要求針對得識別特定人之屬人或屬事事項之各別資訊，應分開儲存。而於不同之各別情況中，究竟應選擇何種具體措施，仍須依據 GDPR 第 35 條進行個資保護影響評估（Datenschutz-Folgenabschätzung）之結果決定之。

然而，此一揭示於德國個資法第 22 條第 2 項「採行適當特定措施」之誡命，是否僅存在於特種個人資料之處理？德國個資法第 22 條第 2 項在體系上雖是針對特種個人資料之處理，且其於德國個資法中，亦多被援用為處理特種個人資料之合法要件之一[239]，但其亦被援用為一般個人資料之目的外處理（德國個資法第 23 條第 2 項及第 24 條第 2 項）之要件，若進一步同時觀察 GDPR 第 32 條第 1 項對於處理一般個人資料所定安全維護要求，與德國個資法第 22 條第 2 項實多有相似之處，包括就選定措施時應關注之面向（GDPR 第 32 條第 1 項；德國個資法第 22 條第 2 項）、個人資料之假名化及加密（GDPR 第 32 條第 1 項第 a 款；德國個資法第 22 條第 2 項第 6 款及第 7 款）、處理個資系統及服務之運作型態與因應能力（GDPR 第 32 條第 1 項第 b 款及第 c 款；德國個資法第 22 條第 2 項第 8 款），以及採行監管處理個人資料安全性之相關措施（GDPR 第 32 條第 1 項第 d 款；德國個資法第 22 條第 2 項第 9 款），故透過與 GDPR 中就處理一般個人資料所規範之要件進行對照，應可認為其適用不應全然限於處理特種個人資料之情況[240]，而亦應得適用於一般個人資料。但可確定者為，處理一般個人資料與特種個人資料，確實會產生採行不同程度及形式「適當特定措施」

[239] 例如：基於就業關係之目的處理勞動者之特種個人資料（德國個資法第 26 條第 3 項）、基於科學或歷史研究目的以及統計目的之處理特種個人資料（德國個資法第 27 條第 1 項）、基於公共利益之檔案儲存目的處理特種個人資料（德國個資法第 28 條第 1 項）以及針對自動化決定之作成而處理健康資料（德國個資法第 37 條第 2 項）之情形，均以德國個資法第 22 條第 2 項作為合法處理特種個人資料之要件之一。

[240] Kühling/Buchner, DS-GVO, BDSG Kommentar, 2. Auflage, 2018, S.1365-1366.

之需求[241]，而具體之步驟及作法，德國之聯邦及邦層級之監督機關共同訂定「個人資料保護模式之標準（Standard-Datenschutzmodell, SDM）」[242]，以資依循。

四、 特殊處理情形

GDPR 第 9 章（第 85 條至第 91 條）中分別針對個人資料保護與言論及資訊自由（第 85 條）、官方檔卷之公開（第 86 條）、國家代碼之處理（第 87 條）、勞動者資料之處理（第 88 條）以及基於公益之檔案儲存目的、基於學術或歷史研究目的以及統計目的之處理（第 89 條）等個人資料處理之特殊情形，為進一步之規範。但因其中置入大量的不確定法律概念以及概括條款，並藉由利益權衡之方式，留給各會員國立法者後續形塑其內國個人資料保護法制時，相當大的形成空間。因此，即便歐盟採用「規則」之立法形式，但其實質內涵，仍有待各會員國之立法者進一步具體詮釋，而使 GDPR 有指令化之趨勢，而仍須仰賴後續各會員國之立法者，方可能有所進展，但亦使得 GDPR 與各會員國法制間的互動與交互影響，受到高度關注[243]。

德國個資法針對GDPR中所定特殊處理之情況，一方面予以深化，訂定更細部之規範，包括：勞動者資料之處理（德國個資法第 26 條）、基於學術或歷史研究目的以及統計目的之處理（德國個資法第 27 條）、基於公益之檔案儲存目的之處理（德國個資法第 28 條）；其次，針對消費借貸過程中之資料處理（德國個資法第 30 條）以及針對為決定是

[241] Eßer/Kramer/v. Lewinski(Hrsg.), DSGVO BDSG Kommentar, 6. Auflage, 2018, S.1484.

[242] Standard-Datenschutzmodell ,https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.1.pdf（德文版）；https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf（英文版）（最後瀏覽日：2020/05/05）

[243] Benecke /Wagner, Öffnungsklauseln in der Datenschutz-Grundverordnung und das deutsche BDSG- Grenzen und Gestaltungsspielräume für ein nationales Datenschutzrecht, DVBl 10/2016, S.604-608. Kühling/Martini, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? EuZW 12/2016, S. 449-450. Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, 5. Aufl., 2014, S. 175.

否簽訂、執行或終止契約，而預測其未來特定行為發生之概然率數值（Scoring），以及關於償付能力及意願概然率數值的查詢(Bonitätsausküften)（德國個資法第 31 條），德國個資法亦將其列屬特殊處理個人資料之情形，應為德國個資法針對經濟活動中處理個人資料進行評等與決策之行為，另行訂定之規範；最後，則是在德國個資法第 4 條中，針對於公眾得出入之場所架設監視器，定有一般性規定，作為公務單位或非公務單位設置監視器時之法律依據。但應注意者為，若前述行為，係以「自動化」之方式作成，則應適用德國個資法第 37 條關於「自動化作成決定」之規定[244]。

(一) 於公眾得出入之場所架設監視器（德國個資法第 4 條）

針對設置監視器之一般性規定，一直得見於德國個資法[245]，德國因應 GDPR 施行所制定之新個資法中，仍針對在公眾得出入場所架設錄影監視設備予以規範，相較於舊法，內容僅作微幅調整。德國個資法第 4 條針對在公眾得出入之場所（öffentlich zugängliche Räume）設置監視器，訂定一般性之規定，其適用對象同時及於聯邦層級之公務單位及非公務單位。若監視器設置之地點，並非屬於公眾得出入之場所，則應回歸適用同法就處理個人資料所訂定之一般性要件[246]。依據德國個資法第 4 條，聯邦機關因為履行其任務、為踐行家主權（Hausrecht）或出於具體確定之目的而為保護正當利益時，方得於公眾得出入之場所設置監視器，除此之外，其同時皆須通過比例原則中「必要性」之檢證[247]，以及透過利益之權衡加以檢證，僅有在當事人值得保護之利

[244] 於 GDPR 立法前言第 71 點中，針對自動化作成決定所為例示，包括線上貸款之拒絕，線上招募程序之拒絕，只要是以自動化之方式作成決定，即受 GDPR 第 22 條之拘束。

[245] 昔日係規定於舊德國個資法第 6b 條。

[246] Kühling/Seidel/Sivridis, Datenschutzrecht, 3. Aufl., 2015, S. 241-244. 德國各邦亦訂定有各邦之個人資料保護法（Landesdatenschutzgesetz），惟其多亦循聯邦個人資料保護法之規範模式與要件，

[247] 於此多會輔以個人資料保護法制中「資料免除（Datenvermeidung）」及「資料縮減(Datensparsam)」等要求予以審視。Kühling/Seidel/Sivridis, Datenschutzrecht, , 3. Aufl., 2015, S. 590.

益未具備應受優先保障之充分事由時，方得為之，當事人利益值得保護之程度，往往會隨著其涉及之權利類型與採行之侵害手段，而有不同之評價，例如對於私密空間之監視或採行不間斷監視之情況，多會於利益權衡時，提升當事人之保護程度[248]。對於多數聯邦機關而言，其多係出於維護自身安全之考量，而於機關所在之建築及其周遭架設監視器。而針對架設於特定處所之監視器，包括公眾所得近用之幅員廣大設施，例如運動場、集會或娛樂場所、購物中心或停車場等，或是設置於交通工具及公眾所得近用之幅員廣大之公共火車、船舶及巴士站等之監視器，對於停留於上述地點之人的生命、健康及自由之保護，應在利益權衡之過程中，將其視為特別重要之利益（德國個資法第 4 條第 1 項）。

為確保當事人之資訊自決權，並提升監視器設置之透明性，德國個資法第 4 條第 2 項要求設置單位應以適當之方式，使人知悉監視之情況及負責單位之名稱與聯絡資料。而針對監視器所蒐集之資料，其後續之處理及利用行為，必須以達成蒐集目的所必要者為限，同時未有事由足認當事人值得保護之利益應為優先時，方得為之。若有目的外之處理或利用之需求，德國個資法第 4 條第 3 項第 3 句將其限於以防止國家或公共安全之危害或為追訴犯罪所必要之情況，方得為之，例如：調閱百貨公司原先基於防盜目的所架設監視器之畫面，作為搜捕對百貨公司內顧客發動攻擊者之用，若其係屬必要之證據時，則應得許其於目的外為處理[249]。另外，由於立法者就此處所稱「犯罪」，並未區分其類型，為避免目的外利用之範圍不成比例之擴張，在體系解釋上，進行目的外之利用前，仍須依據同條第 1 項進行法益之權衡[250]。因此，針對特定地點監視器之設置，應將停留於該處之人的生命、健

[248] 例如於聯邦政府提案之理由中，曾提出若以預防竊盜為由，於更衣間或廁所架設監視器之作法，即非合理之利益權衡結果。Vgl. BT-Drs. 14/5793, S. 62. Scholz, in: Kommentar zum BDSG, 8. Aufl., 2014, S. 747-748.

[249] Kühling/Seidel/Sivridis, Datenschutzrecht, , 3. Aufl., 2015, S.247.

[250] Scholz, Kommentar zum BDSG, 8. Aufl., 2014, S.757.

康及自由納入特別考量之要求，於處理及利用該等資料時，皆有其適用。

錄影監視所蒐集之資料若需與特定當事人進行比對，原則上應依GDPR 第 13 條及第 14 條通知該當事人(德國個資法第 4 條第 4 項)[251]。另外，針對資料保存期限之規定，德國個資法第 4 條第 5 項明定，一旦該資料對於目的之達成已無必要，或繼續儲存違反當事人值得保護之利益時，應立即刪除之，此處之「立即」，應是確認前述刪除要件是否存在所需之作業時間，其雖未明確指明其期間，惟觀諸其立法理由之說明，則認 1 至 2 個工作天當屬已足[252]。而對於前述義務之違反，德國個資法雖未有明文之罰則規定，但其仍得透過相應之制度配套為監督：首先，得由當事人積極主張刪除權，並於受有損害時，請求賠償，另外，其亦得向監督機關提起異議或申訴；同時，德國個資法第 8 條所定之監督機關亦得透過相關監管措施之採行，包括：限期改正或是命其停止監視器之運作並刪除資料等，確保法規之遵循[253]。

(二) 基於就業關係之目的處理資料（德國個資法第 26 條）

依據 GDPR 第 88 條第 1 項之授權，德國立法者於德國個資法第 26 條針對就業關係（Beschäftigungsverhältnis）中勞動者（Beschäftigte）個人資料之處理，其中亦包括特種個人資料之部分，為進一步之規定。德國個資法第 26 條第 8 項針對適用本法之勞動者，劃定其範疇，包括：勞工，涵蓋臨時工（第 1 款）；為了職業教育而工作（第 2 款）；為了參與勞動生活、參與職業傾向之確認或參與試作而提供勞務之參與者（重返就業者）（第 3 款）；於經認可之機構為身心障礙者工作（第 4 款）；依據青少年自願服務法（Jugendfreiwilligendienstgesetz）或聯邦自願服務法（Bundesfreiwilligendienstgesetz）提供自願服務者（第 5 款）；

[251] 於此應一併關注德國個資法第 32 條之適用。
[252] BT-Drs. 14/5793, S. 63. Kühling/Seidel/Sivridis, Datenschutzrecht, , 3. Aufl., 2015, S.247. Scholz, Kommentar zum BDSG, 8. Aufl., 2014, S.760.
[253] Scholz, Kommentar zum BDSG, 8. Aufl., 2014, S.766.

因經濟上之獨立性而被視為具有類似雇主地位者，包括在家工作及與其相當者（第 6 款）以及聯邦公務員、聯邦法官、軍人及服替代役者（第 7 款）[254]。而針對應徵前述工作之應徵者，以及前述就業關係已終結之人均視為本法所稱勞動者[255]。由此可知，德國個資法第 26 條所欲拘束之對象，包括所有在就業關係之脈絡下，處理勞動者所屬個人資料之控管者，包括公務單位及非公務單位，且不僅限與勞動者簽訂契約之雇主，亦包括外部之服務提供者，例如就業服務機構，而代表勞動者之利益團體或工會，其處理所屬勞動者個人資料之行為，亦應受其拘束[256]。德國個資法第 26 條第 5 項進一步強調，針對 GDPR 第 5 條所定基本原則，控管者應採行適當措施，確保其於個人資料之處理中被遵守[257]。

德國個資法第 26 條第 1 項規定了二類處理勞動者個人資料之情況：其一，當處理勞動者之個人資料對於決定成立就業關係，或於成立就業關係後之契約履行或終止，或勞動者權益代表為主張或履行依據本法或團體協約所享有之權利及義務所必要者[258]，得基於就業關係目的處理勞動者之個人資料（德國個資法第 26 條第 1 項第 1 句）。其二，係當經記錄之事實上證據顯示，當事人於就業關係中有犯罪之嫌疑，而該處理係屬舉發犯罪所必要且勞動者就排除個人資料處理並未享有更值得保護之利益，特別是其方式及範圍與其動機間並未不合比例時，得為舉發犯罪處理勞動者之個人資料[259]。（德國個資法第 26 條第 1 項第 2 句）

---

[254] 針對邦或鄉鎮之公務員及法官，由於聯邦就此欠缺立法權，故未規定於聯邦個資法中，而係由各邦之個資法加以規範。另外，由於德國自 2011 年 7 月 1 日起廢除徵兵制，故本條規定適用於替代役之情況，自多屬年代久遠之「舊案」，Sydow(Hrsg.), Bundesdatenschutzgesetz, 2019, S.309.

[255] 此一對於「勞動者」之定義規定，亦得見於舊聯邦個資法第 3 條第 11 項中，然而，其與 GDPR 第 88 條第 1 項所稱「勞動者」是否相符，針對自願服務者（第 5 款）以及類似雇主者（第 6 款），即多有爭論。Sydow(Hrsg.), Bundesdatenschutzgesetz, 2019, S.307.

[256] Sydow(Hrsg.), Bundesdatenschutzgesetz, 2019, S.310.

[257] 此一要求亦得見於 GDPR 第 88 條第 2 項中。

[258] 例如德國個資法第 26 條第 6 項所稱「勞動者權益代表之參與權」，應即屬之。

[259] 此規定得見於舊德國個資法第 32 條第 1 項第 2 句。

若係依據當事人之同意處理勞動者之個人資料，考量就業關係中地位不對等之情況，於判斷該同意是否為自願提供時，德國個資法第 26 條第 2 項強調應特別關注就業關係中勞動者之從屬性以及給予同意之環境。但針對勞動者因此而取得法律上或經濟上優勢或雇主與勞動者所追求法益相同時，應得認定屬出於自願提供同意。除非因特殊情況而以採用其他形式較為適當，同意得以書面或電子之形式為之，例如以電子郵件、Whatsapp 之訊息，均足以當之[260]。另，雇主應向勞動者以文字形式說明關於資料處理之目的及其依據 GDPR 第 7 條第 3 項得主張之撤回權。

針對勞動者之特種個人資料，德國個資法第 26 條第 3 項鬆綁 GDPR 第 9 條第 1 項對於特種個人資料處理之限制，就為達成就業關係之目的，允許處理特種個人資料，當其係為行使權利或履行勞動法上之法定義務、社會安全及社會保護所必要，且未有理由足認，有當事人因排除該處理所得獲致之法益較值得保護之例外情況。基於就業關係之目的處理勞動者之特種個人資料，亦得依據當事人之同意或團體協約為之[261]，而對於特種個人資料處理之當事人同意，應依據德國個資法第 26 條第 2 項之規定予以判斷，且該同意必須清楚地指明欲處理之資料。德國個資法第 26 條第 3 項第 3 句並要求控管者針對處理特種個人資料之情形，應採行同法第 22 條第 2 項所定適當之特定措施，以確保當事人之權益。

德國個資法第 26 條第 7 項主要係將以非自動化方式處理勞動者之個人資料之情形納入規範，亦即所謂類似已儲存之個人資料（analog

[260] 2019 年德國個資法修法時，為適度降低取得當事人同意之難度，將德國個資法第 26 條第 2 項第 3 句原先「同意應以書面為之」之規定，改為「應以書面或電子之形式為之」，亦與 GDPR 第 4 條第 11 款取得一致性。BT-Drs. 19/1181, S.7.

[261] 德國個資法第 26 條第 4 項規定：「個人資料之處理，包括基於就業關係之目的處理勞動者之特種個人資料，得依據團體協約為之。於此談判者應留意 GDPR 第 88 條第 2 項。」

gespeicherter Daten）[262]或未上線（off-line）之個人資料，包括：手寫記錄，如：對於求職對談之註記；以口頭或隨機方式處理個人資料，如：致電前雇主確認其所簽發之工作證明書；事實上之行為，如：出入管制之紀錄等。本項規定擴張了 GDPR 第 2 條第 1 項所定之適用範圍，將處理勞動者各種個人資料之各類型態，無論其係處理一般個人資料或特種個人資料，不論其屬全自動化、部分自動化或非自動化處理，一體要求應遵循德國個資法第 26 條所規範之要件[263]。但其應仍有其限度，例如一般社會常見之資料處理，像是問候「您週末過得如何？」，即不應落入德國個資法第 26 條之適用範圍[264]。

(三) 基於科學或歷史研究目的以及統計目的之資料處理（德國個資法第 27 條）

德國個資法第 27 條排除 GDPR 第 9 條第 1 項對於處理特種個人資料之限制，若屬為達成科學或歷史研究目的以及統計目的所必要，且控管者處理個人資料所獲致之利益顯然高過於當事人排除該處理所得獲致之法益時，即便未取得當事人之同意，亦得處理特種個人資料。控管者應依據德國個資法第 22 條第 2 項第 2 句採行相應之適當並特定之措施[265]，以維護當事人之法益。（德國個資法第 27 條第 1 項）

由於 GDPR 在權衡研究與統計目的以及個人資料保護後，於 GDPR 第 89 條第 2 項授權各會員國得針對基於研究與統計目的處理個人資料之行為，得自行制定內國法令限制當事人權利之行使，藉由限縮當事人所得主張之權利，創設對基於前述目的處理個人資料之有利條件，促進個人資料之合理利用[266]。德國個資法第 27 條第 2 項第 1 句即據此

[262] 類似已儲存之個人資料（analog gespeicherter Daten）之概念得見於德國個資法第 32 條第 1 項第 1 款之要件中。
[263] 舊德國個資法第 32 條第 2 項亦得見相同之規定。
[264] Sydow(Hrsg.), Bundesdatenschutzgesetz, 2019, S.330-331.
[265] 請參考前述（三）去識別化之要件、程序、認定方式等規定中之說明。
[266] 李寧修，個人資料合理利用模式之探析：以健康資料之學術研究為例，臺大法學論叢，49 卷 1 期，2020 年 3 月，頁 32-33。

對於當事人依據 GDPR 得主張之近用權(第 15 條)、更正權(第 16 條)、限制處理權（第 18 條）及拒絕權（第 21 條）加以限制：針對該權利之主張可能造成研究或統計目的無法達成或導致重大妨礙，且限制前述權利係屬達成該目的所必要時，則當事人不得主張之[267]。另外，特別針對 GDPR 第 15 條之近用權，當個人資料係屬達成科學研究目的所必要，且提供查詢可能須耗費不成比例之費用時，當事人不得依據 GDPR 第 15 條主張近用權。(德國個資法第 27 條第 2 項第 2 句）

德國個資法雖循 GDPR 之方向，放寬基於研究或統計目的處理個人資料之要件，但同時亦要求應採行相關之配套，以維護當事人之自由與權利，德國個資法第 27 條第 3 項針對基於研究或統計目的處理特種個人資料之情形，除要求應採行德國個資法第 22 條第 2 項對於處理特種個人資料所定適當且特定措施外，應於研究或統計目的允許之範圍內，予以匿名化（zu anonymisieren)，但該匿名化若與當事人之正當利益有所衝突，則不在此限。而於匿名化前，針對得識別特定或可得特定人之屬人或屬事之個別資料，應分開儲存。在達成研究或統計目的所必要之範圍內，方得允許將個別資料加以彙整。

控管者得公開個人資料，但須經當事人同意或其係呈現與時代歷史重大事件相關之研究成果所絕對必要者，方得為之（德國個資法第 27 條第 4 項)。

(四)　基於公共利益之檔案儲存目的之資料處理(德國個資法第 28 條）

德國個資法第 28 條開啟了基於公共利益之檔案儲存目的之，處理特種個人資料之可能性，鬆綁了 GDPR 第 9 條第 1 項對於特種個人資料處理之限制，一旦屬為達成公共利益之檔案儲存目的所必要，即允許得處理特種個人資料。由於本條亦係在規範對於特種個人資料之處理，故同時連結德國個資法第 22 條第 2 項第 2 句，要求控管者應採行

[267] 此要件亦得見於 GDPR 第 89 條第 2 項。

相應之適當並特定之措施，以維護當事人之法益。（德國個資法第 28 條第 1 項）

當檔案並非透過當事人之姓名作成，或並未提供得以合理之行政費用查找相關檔案之資料時，德國個資法第 28 條第 2 項對於當事人依據 GDPR 第 15 條得主張之近用權予以排除。本條規定係為確保檔案之功能得以正常運作，而不致因當事人提出查詢，而負有將全部檔案進行搜尋與整理之義務[268]，此一規定亦得見於特別法中，例如聯邦檔案法第 14 條第 1 項即屬適例。

當個人資料係基於公共利益之檔案儲存目的為處理時，德國個資法第 28 條第 3 項明定當事人不得依據 GDPR 第 16 條主張更正權。但當事人若對於個人資料之正確性有疑義，應給予其表達不同意見之機會，以為衡平[269]。專責檔案機關負有將該不同意見附加於資料之義務。但對於個人資料正確性之意見，應限於事實部分，個人意見之表述則不屬之[270]。

GDPR 第 89 條第 3 項授權各會員國針對基於公共利益之檔案儲存目的之資料處理，得藉由制定內國法以限制當事人權利之行使，包括：GDPR 第 15 條近用權、第 16 條之更正權、第 18 條之限制處理權、第 19 條之通知義務、第 20 條之資料可攜權以及第 21 條所定之拒絕權。德國立法者承接 GDPR 之授權，於德國個資法第 28 條第 4 項進一步對於 GDPR 第 18 條第 1 項第 a 款（對於個人資料正確性有疑義）、第 b 款（不合法之處理）及第 d 款（對個人資料之處理表達異議）限制處理權之主張，第 20 條資料可攜權及第 21 條拒絕權之行使，若其可能對於基於公共利益之檔案儲存目的無法達成或導致重大妨礙，則當事人不得主張之，但該限制應以達成目的之必要範圍為限。

---

[268] Sydow(Hrsg.), Bundesdatenschutzgesetz, 2019, S.345.
[269] 聯邦檔案法第 14 條第 4 項亦得見相同之規定。
[270] Sydow(Hrsg.), Bundesdatenschutzgesetz, 2019, S.345.

(五) 消費借貸（德國個資法第 30 條）

德國個資法第 30 條之規定得見於舊德國聯邦個資法第 29 條第 6 項及第 7 項，係為了轉化歐盟 2008/48/EG 指令（消費借貸契約指令）[271]第 9 條之規定而制定，其一方面呼應該指令在消費借貸契約領域保障消費者權益之宗旨（德國個資法第 30 條第 2 項），同時亦以確保市場公平競爭為目的（德國個資法第 30 條第 1 項）[272]。

德國個資法第 30 條第 1 項針對單位之業務上個人資料，係得利用於消費者之信用評等，基於傳遞之目的而為蒐集、儲存或變更，對於來自歐盟其他會員國之貸與人所提出查詢請求，應與本國之貸與人受相同待遇[273]。

德國個資法第 30 條第 2 項透過課予消費借貸貸與人告知之義務，提高消費信用契約訂約過程之透明性，以確保消費者之權益，可被視為強化 GDPR 告知義務之規定。若欲與消費者簽訂消費借貸契約或關於有償財務紓困契約，卻因德國個資法第 30 條第 1 項所稱單位所提供之查詢結果而予以拒絕時，應立刻通知消費者以及其所收到之查詢結果。但若拒絕消費借貸契約之理由，並非因消費信用之查詢結果所致，而是透過關於償付能力及意願概然率的查詢(Bonitätsausküften)，而予以拒絕時，則該通知義務則因與德國個資法第 30 條第 2 項所定要件未符而不存在。該通知義務係加諸於消費借貸契約之貸與人，而非提供信用評等查詢之單位[274]。該告知不得收費並應附具理由[275]，而通知之

[271] 關於歐盟 2008/48/EG 消費信用契約指令，請參考 https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008L0048:de:HTML（最後瀏覽日：2020/05/05）

[272] Sydow(Hrsg.), Bundesdatenschutzgesetz, 2019, S.354.

[273] 但其並未要求給予較佳之待遇，因此，立法理由亦明確指出，對於本國貸與人請求查詢時收取費用之要求，對於來自其他會員國之貸與人亦應一體適用。Vgl. BT-Drs. 16/11643, S. 140.

[274] 實務上常發生貸與人以及提供信用評等單位相互卸責之情況，尤其是當實際處理個人資料之控管者應為提供信用評等單位，然而告知義務卻主要由貸與人擔負，而與個人資料保護法制中對於告知義務之課予，有較為不同之思考面向。Sydow(Hrsg.), Bundesdatenschutzgesetz, 2019, S.359.

期限應可參照德國民法第 121 條所稱「無過失之遲延」加以認定，另外，於該期限亦應允許就該告知是否符合個人資料保護相關規範，進行審核[276]。然而，一旦通知可能造成公共安全或秩序之危害時[277]，則免除通知義務。

(六) 於計分及支付能力查詢之經濟交易保護（德國個資法第 31 條）

德國個資法第 31 條整併了舊德國個資法第 28a 條及第 28b 條之規定，其係以保護經濟交易為目的[278]，規範計分（Scoring）數值之使用（德國個資法第 31 條第 1 項），以及進一步將該計分數值用於支付能力查詢(Bonitätsausküften)時，所應遵循之要件（德國個資法第 31 條第 2 項）。所謂「計分」，係指基於與特定人簽訂、執行或終止契約之目的，對其未來特定行為發生概然率之數值，計分本身必須以合法蒐集之個人資料為其基礎，而計分數值之使用，則必須進一步符合德國個資法第 31 條所定要件。由於 GDPR 就此並未有相關之規定或授權條款，或許得藉由 GDPR 第 22 條第 2 項第 b 款連結第 23 條第 1 項第 e 款，開啟歐盟各會員國自行立法規範之可能性[279]。

德國個資法第 31 條第 1 項針對基於與特定人簽訂、履行或終止契約之目的，使用對其未來特定行為發生概然率數值，即所謂計分，僅得於下列各款要件均符合時，方得為之。

－遵守個人資料保護法制之規定，

---

[275] Vgl. BT-Drs. 16/11643, S. 140.
[276] Sydow(Hrsg.), Bundesdatenschutzgesetz, 2019, S.359.
[277] 故若係對於營業秘密或職務秘密之危害，恐仍不足以當之。Sydow(Hrsg.), Bundesdatenschutzgesetz, 2019, S.360.
[278] Vgl. BT-Drs. 16/11325, S. 101.
[279] 但有論者指出，德國個資法第 31 條係針對使用計分數值之要件，但「對當事人相應產生法律效果或產生類似之重大影響」，應非「使用計分數值」此一處理個人資料行為本身所造成，而係「使用計分數值後所得出之結果」所帶來的影響，故其是否符合 GDPR 第 22 條第 1 項之要件，而得以同條第 2 項為其基礎，即不無疑義。Sydow(Hrsg.), Bundesdatenschutzgesetz, 2019, S.363.

－計算概然率數值所利用之個人資料係依據有科學認可之數學統計方法證明計算該特定行為之概然率數值屬顯著，

－概然率數值之計算並未僅利用地址資料，

－於利用當事人地址資料之情形，已於計算概然率數值之前即已通知其預計利用該等資料之情形；該通知應紀錄之。

德國個資法第 31 條第 2 項進一步針對於取得有關債權資訊之情況，將查詢機構（Auskunfteien）所提供之概然率數值使用於調查自然人償付能力及意願時，除應具備德國個資法第 31 條第 1 項所定要件，且該債權限於債務屆期未履行之情形，並符合下列要件之一，方得為之：

－其由確定判決或目前宣告執行之判決所確認或依據民事訴訟法第 794 條具有債務名義，

－符合破產法第 178 條且於審查期日未為債務人所爭執

－經債務人明確承認，

－就此已對債務人於屆期後至少為二次書面警告；第一次警告至少於四週前作成；債務人先前，但最早於第一次警告時，已由詢問機構告知可能之注意事項；債務人對此債權並不爭執，

－其所依據之契約關係由於延遲繳納得不受期限拘束解除且債務人先前就可能應注意之事項已經詢問機構通知。

五、 自動化機器做成之決定

對於藉由自動化方式作成之決定，且其對當事人將產生法律上效果或重大影響時，GDPR 第 22 條第 1 項賦予當事人抵禦之權利，原則上禁止於個案中採行自動化決定，以防免當事人因此遭受到不利之法律效果或以類似之形式受到重大影響，但同條第 2 項中，其亦規範三

種得例外採行之情形。德國立法者即透過 GDPR 第 22 條第 2 項第 b 款之授權[280]，於德國個資法第 37 條中，針對 GDPR 第 22 條第 2 項中「履約所必要（第 a 款）」以及「經當事人明確同意（第 c 款）」二種例外得為自動化決定之情形，將其適用範圍限縮於「依據保險契約提供給付」之範圍內[281]，且必須符合以下要件之一：

－該要求已經當事人允許（德國個資法第 37 條第 1 項第 1 款）。

－該決定與實施對治療行為具拘束力之收費規定有關，且控管者對於該申請並未獲得充分同意之情形，採取適當之措施以維護當事人之正當利益，於此至少包括獲知代表資料控管者涉入之人的權利、陳述自身觀點之權利以及撤銷該決定之權利；[282]資料控管者至遲於獲知該申請未獲當事人充分同意之時，通知當事人關於該等權利（德國個資法第 37 條第 1 項第 2 款）。

一旦保險契約給付及於第三人，考量於此自動化決定程序中亦會處理該第三人之個人資料，故德國個資法第 37 條第 1 項第 2 款所定告知義務，亦應及於該第三人[283]。

針對自動化決定之作成，德國個資法第 37 條第 2 項允許處理健康資料，但對於健康資料之範圍，限於 GDPR 第 4 條第 15 款所定義者，故並未涵蓋基因資料（GDPR 第 4 條第 13 款）或生物資料（GDPR 第 4 條第 14 款）。但控管者於此必須相應採行德國個資法第 22 條第 2 項中所舉維護當事人法益之適當且特定的措施。此亦屬德國立法者依據 GDPR 第 9 條第 2 項第 g 款，對於健康資料之處理，於德國個資法中

[280] GDPR 第 22 條第 2 項第 3 款允許各會員國以其內國法令訂定得採行自動化決定之個案情形。另一適例則為德國行政程序法第 35a 條之規定，其明定於全自動之行政程序中，得自動化作成行政處分之要件。Vgl. BT-Drs. 18/11325, S. 106.

[281] 德國立法者於立法理由中，即不諱言地指出，該條係以保障「保險產業之特殊利益」為目的。Vgl. BT-Drs. 18/11325, S. 106.

[282] 同 GDPR 第 22 條第 3 項

[283] Sydow(Hrsg.), Bundesdatenschutzgesetz, 2019, S.431.

所制定之特別規範。

六、 當事人權利

相較於 GDPR 第 8 條針對兒童作為當事人主體適格性所建立之認定標準，德國個資法就此未有明文，故將適用 GDPR 之規定，但關於兒童得否以當事人同意提供個人資料，實務上多主張與民法之行為能力切割觀察，而必須依據兒童之年齡、生活經驗及理解能力等進行個案認定，強調應將重點置於兒童對提供個人資料行為所代表之法律上意義及效果，包括蒐集之目的、後續利用之範圍，以及其作為當事人所得主張之權利...等，是否具有充分的理解與認知能力，而未必受限於特定年齡[284]。

德國個資法第 32 條至第 37 條，針對當事人權利之部分予以細節化之規範，但相當特別的是，其主要係依據 GDPR 第 23 條賦予各會員國之權限，以內國法限縮 GDPR 所規定當事人權利適用之要件，其中包括：GDPR 第 13 條及第 14 條之告知義務、第 15 條之近用權、第 17 條之刪除權及第 21 條之拒絕權。

(一) 告知義務

1. 直接蒐集而為後續處理之告知義務（德國個資法第 32 條）

德國個資法第 32 條針對 GDPR 第 13 條第 3 項對於直接向當事人蒐集而為後續處理之告知義務，明定五種特殊情況，免除再處理時控管者之告知義務：

－對於類似已儲存個人資料（analog gespeicherter Daten）之再處理，若控管者係透過再處理直接將該資料用於當事人，且該再處理之

[284] 此與 GDPR 第 12 條第 1 項強調對於兒童所為告知，更應特別注意其是否對於兒童屬明確易懂之要求，不謀而合。而此一判斷，即有待於個案中為之。

目的與原始蒐集目的具有一致性[285]，且其與當事人之溝通並非運用數位形式（in digitaler Form），而當事人於因告知所得獲致之法益，以資料蒐集之整體關聯性觀察，於各別情況中屬較為輕微者（第 32 條第 1 項第 1 款）。所謂「類似已儲存之資料」，於德國個資法中並未加以定義，立法理由中亦未見相關說明，但考量本款規定主要係針對資料處理尚未全面或僅小部分電子化之中、小型企業，為減輕其負擔而為之規定，故其適用應限於非以數位形式處理或尚未電子化之個人資料，其較可能屬記載於例如：索引卡、顧客卡、紙本檔案等載體中之個人資料，因此自動化作成之資料應即非屬本款所涵蓋之範圍。而該後續處理，應亦限於非數位形式[286]。但隨著數位處理技術之發展與普及，本款適用之情況應會逐漸減少，因而較屬於過渡期之緩衝規定。

－對於公務單位作為控管者，依法履行與 GDPR 第 23 條第 1 項第 a 款至第 e 款相關之職務可能造成危害，且其不告知所得維護之法益，較當事人之法益值得保護者（德國個資法第 32 條第 1 項第 2 款）。本款規定僅適用於公務單位，針對告知義務之履行，可能造成依法執行職務之危害，其涵蓋之範圍甚廣，包括國家安全（GDPR 第 23 條第 1 項第 a 款），國家防衛（GDPR 第 23 條第 1 項第 b 款），公共安全（GDPR 第 23 條第 1 項第 c 款），預防、調查、偵查或追訴犯罪或執行刑罰（GDPR 第 23 條第 1 項第 d 款）以及保障歐盟或會員國一般公共利益之重要目的（GDPR 第 23 條第 1 項第 e 款）等。由於前述法益多屬抽象而留有判斷餘地，故適用上強調其所造成之危害應屬有客觀事實足認之具體危害，單純之臆測或僅屬風險，並不足以當之，且該等危害之造成必須與告知義務間具有因果關係，本款並定有利益權衡條款，故須經過利益權衡加以確

[285] GDPR 第 6 條第 4 項參照。
[286] Sydow(Hrsg.), Bundesdatenschutzgesetz, 2019, S.377.

認後，方得免除公務單位之告知義務[287]。

－妨害公共安全或秩序或對於聯邦或邦之福祉（Wohl）可能招致不利益，且控管者因不告知所得維護之法益，較當事人之法益更值得保護者（德國個資法第 32 條第 1 項第 3 款）。透過立法意旨可知，本款規定亦僅適用於公務單位[288]，其所欲維護之「公共安全」與「公共秩序」之概念，因亦屬不確定法律概念，故於個案之判斷，多會參照亦大量援用此等概念之警察與秩序法[289]，且亦須經過利益權衡加以確認。惟針對「公共秩序」之妨害，與德國個資法第 32 條第 1 項第 2 款中所指涉之 GDPR 第 23 條第 1 項第 e 款之規定有所重疊，在適用上應如何選擇，恐仍有待釐清。

－對於法律上請求權之適用、行使或防衛，可能造成妨害，且控管者因不告知所得維護之法益，較當事人之法益值得保護者（德國個資法第 32 條第 1 項第 4 款）。本款規定對於公務及非公務單位皆有其適用，其主要係基於 GDPR 第 23 條第 1 項第 j 款而訂定，但並未如 GDPR 侷限於民事上之請求權，其於訴訟程序中或訴訟程序外，均有其適用，但仍須經過利益權衡加以確認[290]。

－可能造成向公務單位秘密傳輸資料之妨害（德國個資法第 32 條第 1 項第 5 款）。本款所欲保障之法益，除維護向公務單位傳輸個人資料之秘密性外，同時亦被視為吹哨者保護條款（Whistleblowerschutz），即當私人欲向公務單位舉發特定事件或人，甚至是在刑事追訴程序中，對於其中所涉及個人資料所為之再處理，免除告知之義務[291]。

針對控管者因德國個資法第 32 條第 1 項第 1 款至第 3 款因而免除

[287] Sydow(Hrsg.), Bundesdatenschutzgesetz, 2019, S.381.
[288] Vgl. BT-Drs. 18/11325, S.103.
[289] Sydow(Hrsg.), Bundesdatenschutzgesetz, 2019, S.381.
[290] Sydow(Hrsg.), Bundesdatenschutzgesetz, 2019, S.382.
[291] Schanz/Wolff, Das neue Dayenschutzrecht, 2017, Rn. 1167.

告知義務之情況，德國個資法第 32 條第 2 項要求控管者應相應採行適當措施維護當事人之正當利益，其中包括以更明確、更透明、更易於理解且更易於取得之形式，以清楚並簡易之文辭，對外公開 GDPR 第 13 條第 1 項所定之基本告知事項以及第 2 項之延伸告知事項。控管者對於其得以免除告知義務之原因，應以書面記錄之。

若德國個資法第 32 條第 1 項所定免除告知義務情況之發生，但其原因僅屬暫時性之障礙（vorübergehender Hinderungsgrund）者，控管者於該暫時無法為告知之原因消失後，應適時補行告知，而補行告知之適當期間，不得逾二星期（德國個資法第 32 條第 3 項）。

2. 間接蒐集而為後續處理之告知義務（德國個資法第 33 條）

針對間接蒐集之告知義務，德國個資法第 33 條於 GDPR 第 14 條第 5 項以及德國個資法第 29 條第 1 項第 1 句所定例外之外，進一步增訂了排除 GDPR 第 14 條第 1 項、第 2 項及第 4 項告知義務適用之例外情況：首先，針對公務單位之情形，當告知對於公務單位依法履行與 GDPR 第 23 條第 1 項第 a 款至第 e 款相關之職務可能造成危害（德國個資法第 33 條第 1 項第 1 款第 a 目）；或妨害公共安全或秩序或對於聯邦或邦之福祉可能導致不利益（德國個資法第 33 條第 1 項第 1 款第 b 目）時，且前述二種情況中，當事人因受告知所得獲得之法益，並未於利益權衡中獲致較有利之地位者，則免除公務單位因間接蒐集而為後續處理之告知義務。

其次，針對非公務單位，當該告知可能妨害民事上請求權之適用、行使或防衛，或處理之資料係來自於民事契約中且係為預防因刑事犯罪所生損害，而當事人於受告知所得獲致之正當利益，並未於利益權衡中獲致較有利之地位者(德國個資法第 33 條第 1 項第 2 款第 1 目)；或是經專責公務單位認定，控管者公布資料可能危害公共安全或秩序或可能對於聯邦或邦之福祉招致不利益時（德國個資法第 33 條第 1 項

第 2 款第 b 目前段）[292]，免除非公務單位因間接蒐集而為後續處理之告知義務，但基於刑事追訴目的所為資料處理，則無須經前述公務單位確認。於德國個資法第 33 條第 1 項第 2 款第 b 目有權加以認定之公務單位，應屬負有維護公共安全及秩序或防止對聯邦或邦福祉之不利益義務之機關，非公務單位僅於取得其確認後，方得免除告知義務。

與前述德國個資法第 32 條第 2 項相同，針對因德國個資法第 33 條第 1 項而免除告知義務之情況，德國個資法第 33 條第 2 項亦要求控管者應相應採行適當措施維護當事人之正當利益，其中包括以更明確、更透明、更易於理解且更易於取得之形式，以清楚並簡易之文辭，對外公開 GDPR 第 14 條第 1 項所定之基本告知事項以及同條第 2 項之延伸告知事項。控管者對於其得以免除告知義務之原因，應以書面記錄之。

針對公務單位基於國家安全目的傳遞資料予特定機關，如憲法保護機關、聯邦情報機關、軍事防護勤務單位以及涉及聯邦安全之其他聯邦國防部所屬機關，則關於該傳遞之告知，僅得於獲得該等機關之同意下，方得為之（德國個資法第 33 條第 3 項）。

(二) 近用權

德國個資法第 34 條針對 GDPR 第 15 條以及德國個資法中所定特殊處理情形中之基於科學或歷史研究目的以及統計目的之資料處理（德國個資法第 27 條）、基於公共利益之檔案儲存目的之資料處理（德國個資法第 28 條）以及第 29 條中關於近用權之行使，加以限制。當依據德國個資法第 33 條第 1 項第 1 款、第 2 款第 b 目或第 3 項之規定，無須告知當事人（德國個資法第 34 條第 1 項第 1 款）；或該資料係因依據法律或命令所定儲存規定無法刪除，而因此儲存者（德國個資法第 34 條第 1 項第 2 款第 a 目），或專為達成資料安全或資料保護控管

[292] 此與舊德國個資法第 33 條第 2 項第 6 款之意旨相同。

之目的（德國個資法第 34 條第 1 項第 2 款第 b 目），且該查詢將可能須花費不合比例之費用並採行適當之技術及組織上措施排除目的外處理之可能時，則當事人不得主張近用權。

對於例外拒絕提供當事人查詢之情形，德國個資法第 34 條第 2 項要求應將拒絕查詢之理由予以紀錄，且如告知當事人關於作成拒絕查詢決定之事實上或法律上理由，並不會對拒絕查詢所欲達成之目的造成妨礙時，應即告知當事人該拒絕之理由。為了達成提供當事人查詢之目的以及因就此為準備而儲存之資料，僅得於此目的內以及為資料控管之目的為處理；出於其他目的所為處理，受 GDPR 第 18 條關於限制處理權之限制。

若當事人係遭聯邦之公務單位拒絕提供查詢，且其非屬經聯邦最高專責機關確認，該告知可能妨害聯邦或邦之安全的各別情形時，則其得依請求告知聯邦個人資料保護監察官。由聯邦個人資料保護監察官告知當事人關於個人資料保護法上審查之結果中，若其並非屬廣泛之查詢，不應包含資料控管者判別之推論。

當事人對於其受公務單位既非以自動化方式處理，亦非屬以非自動化方式處理並儲存於資料系統中之個人資料時，僅得於當事人足以釋明該資料可能尋得以及提供查詢所生必要費用未與當事人因公開所得獲致之資訊利益不符比例情況下，方得主張近用權（德國個資法第 34 條第 4 項）。

(三) 刪除權

德國個資法第 35 條第 1 項排除 GDPR 第 17 條第 1 項所定刪除權與第 17 條第 3 項所定例外之適用。若其所欲刪除之個人資料係以非自動方式處理，並依據其特殊之儲存形式無法刪除或需花費不成比例之高額費用方得刪除，且當事人因刪除所得受保護之法益屬較輕微者，則限制當事人刪除權之行使，並免除控管者之刪除義務。然而，於此

所考量之「刪除所需之費用」，是否屬 GDPR 第 23 條第 1 項所明定之法益？不無疑義[293]。德國個資法第 35 條第 1 項雖限制刪除權之主張，但 GDPR 第 18 條關於限制處理權之規定，於此對於免除刪除義務之控管者仍有其適用。但對於刪除權之限制以及限制處理權之主張，均以該個人資料係經合法處理為前提。

GDPR 第 18 條第 1 項第 b 款及第 c 款，於 GDPR 第 17 條第 1 項第 a 款及第 d 款之情況，若控管者有理由認為，刪除將可能導致當事人應受保障之法益受到影響，準用第 1 項第 1 句及第 2 句之規定。就處理之限制，若該通知並非不可能或未顯示可能須耗費不成比例之費用，資料控管者應通知當事人（德國個資法第 35 條第 2 項）。

當刪除與法令或契約所定保留期限相互牴觸時，德國個資法第 35 條第 3 項規定，為了履行法定義務所為處理或為執行達成公共利益之任務或行使公權力（GDPR 第 17 條第 3 項第 b 款），而個人資料之蒐集或處理對於蒐集目的之達成已非屬必要時（GDPR 第 17 條第 1 項第 a 款），準用第 1 項之規定，意即若其所欲刪除之個人資料係以非自動方式處理，並依據其特殊之儲存形式無法刪除或需花費不成比例之高額費用方得刪除，且當事人因刪除所得受保護之法益屬較輕微者，則限制當事人刪除權之行使並免除控管者之刪除義務。

(四) 拒絕權

針對 GDPR 第 21 條賦予當事人之拒絕權，德國個資法第 36 條限縮其得主張之範圍：其一，為當個人資料之處理涉及急迫公共利益之維護，且其較當事人權利更值得保護時，不得主張拒絕權。此與 GDPR 第 23 條第 1 項第 e 款所定法益較為相關，但「公共利益」之範圍是否應受限於 GDPR 第 23 條第 1 項第 e 款下所提及之重要之經濟或財政利益，例如貨幣、預算、稅捐公共衛生及社會安全？若僅以「急迫」作

[293] Sydow(Hrsg.), Bundesdatenschutzgesetz, 2019, S.411.

為唯一之認定標準，恐招致過度限制拒絕權之批評[294]。

其二，則是若該處理係法規明定之義務者，則當事人不得依據 GDPR 第 21 條第 1 項對公務機關提出異議。但由於基於法定義務處理個人資料，屬 GDPR 第 6 條第 1 項第 c 款所定合法處理個人資料之要件，且已透過 GDPR 第 21 條第 1 項之要件排除適用，於此再次重申，似僅屬重複規範而無必要[295]。

除德國個資法第 36 條以外，於基於科學或歷史研究目的以及統計目的處理資料以及基於公共利益之檔案儲存目的處理資料之情形，分別於德國個資法第 27 條第 2 項以及德國個資法第 28 條第 4 項， 就當事人拒絕權之主張亦同有排除適用之規定。

GDPR 第 23 條雖允許各會員國基於維護特定法益，以內國法限制當事人權利之行使，但亦要求該等立法內容必須明確包括下列事項：處理之目的或處理之類型、個人資料之類型、限制之範圍、防制濫用或不合法之近用或移轉之保護措施、對於控管者之說明或其類型、儲存期限以及考量處理之種類、範圍目的或處理類型而為之適當安全維護措施、對於當事人之自由與權利將導致之風險、當事人受告知遭限制之權利。而德國立法者於德國個資法第 32 條至第 37 條對於 GDPR 明定當事人權利所加諸之限制，是否均符合 GDPR 第 23 條之要求，或許仍容有進一步討論之空間[296]。

[294] 就此，聯邦參議院於立法程序中所提出之意見中指出，此規定對於拒絕權之限制非屬必要，亦不符合比例，並主張刪除之。Vgl. BT-Drs. 18/11655, S. 40.

[295] Vgl. BT-Drs. 18/11655, S. 24.

[296] 例如：德國個資法第 35 條似有意迴避其究竟係以 GDPR 第 23 條第 1 項何款為依據，德國個資法第 36 條則對於 GDPR 第 23 條第 2 項所要求應於立法中明確規範之事項，似有欠缺，應屬仍有改善空間。

第四章 臺灣、英國及德國個人資料保護法制之比較、分析

第一節　議題比較

關於 GDPR 與我國個資法之比較，法務部提出「歐盟資料保護一般規則(General Data Protection Regulation，GDPR)與我國個人資料保護法之重點比較分析」之文件中[297]，總結歸納了以下說明（強調部分為本報告增加）：

> 關於 GDPR 之規範內容，在當事人之權利部分，除以往之資料查詢、複製、更正及刪除權之外，更進一步賦予當事人得請求資料控管者及受託處理者刪除連結(被遺忘權)、要求以可共同操作之格式提供資料(資料可攜權)等權利。在資料控管者部分，新增個資保護影響評估、DPO 等制度。惟 GDPR 諸多新穎性規範，實務上究應如何運作，仍待歐盟第 29 條個資保護工作小組持續訂定規範加以補充，我國並應持續密切觀察 GDPR 施行情形以為因應借鑑。

而本報告在進行比較分析時，與其說是將研究中心放在前端眾多論著早已比較過的當事人新權利以及資料控管者新義務，毋寧為後者關於「該等新穎性規範，實務上究應如何運作」之剖陳。

一、 個資保護監管機關

(一) 英國部分

英國資訊委員在深化新法規調適的工作上，較明顯地把重心放在

[297] 法務部，歐盟資料保護一般規則(General Data Protection Regulation，GDPR)與我國個人資料保護法之重點比較分析，https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC8xMTY5NC82N2Q4YmI1YS1kYzJlLTRhNzktYmFkYi1jMWQxNGRlZDc4YzEucGRm&n=5q2Q55ufR0RQUuiIh%2baIkeWci%2bWAi%2bS6uuizh%2baWmeS%2fneitt%2bazleS5i%2bmHjem7nuavlOi8g%2bWIhuaekC5wZGY%3d&icon=..pdf, 頁 7。

宣導、發布相關指引、發布法規命令等。最重要的訣竅在於針對不同需求群體，做出分層分流，目標導向的行動。其次，有效善用 DPO 作為 ICO 與民眾及私人組織的連結，也有其效率性。

而之所以能具體地顯示出調適新法規的效率性，ICO 事實上在 2019 年度新增投入相當地顯著。因此未來倘若臺灣有意設立獨立專責機關，則不但在機關職員任命保障與機關職權獨立上非常地重要，相關人力、預算與場所之資源，亦有其重要性。

(二) 德國部分

德國就個人資料保護採行之監管模式，沿襲指令時代所建構之二根支柱監管模式：一方面藉由課予資料控管者及受託處理者設置 DPO 之義務；另一方面，則是要求各會員國應建立一或多個個人資料保護之專責監督機關，並強調無論是 DPO，抑或監督機關，於行使職權時均應具備之獨立性。針對個人資料保護監督權責之劃分，由於德國係採行聯邦體制，於聯邦層次設有聯邦個人資料保護暨資訊自由監察官，作為最高聯邦機關之一；於邦之層級，則分別設有邦之個人資料保護監察官，另亦有於特定領域之個人資料保護監管，於邦之層級另行設置監察官之例，例如：巴登-符騰堡邦（Baden-Württemberg）之個人資料保護法第 27 條，即於邦個人資料保護監察官外，設置廣電個人資料保護監察官，共同作為邦層級之監督機關。

德國就個人資料保護所建置之監管體系，或可供我國參考者，包括：

－個人資料保護之監督機關應具備獨立性，應屬目前個人資料保護法制中具有高度共識者，於此不再贅言。但考量個人資料保護往往與資訊公開間產生拉鋸，而須進行利益權衡，故德國係將個人資料保護及資訊公開此二項職權之監管，交由同一機關，即聯邦個人資料保護暨資訊公開監察官所執掌。

－針對執掌個人資料保護之監督機關，並非僅有單一機關，而係依據國家體制，分別由聯邦及邦共同擔當，並透過定期性之會議，作為聯邦及各邦監督機關相互溝通、交流之平台。但均要求其須為「專責機關」，亦即該機關之設立，應以專門負責個人資料保護之監管為主。此與我國由中央目的事業主管機關或地方政府作為監督機關之作法，有所不同。

－不論是設於聯邦或邦層級之個人資料保護監察官，均係採行首長制而非合議制，而在邦之層級，即對於特定領域之個人資料保護監管，再行任命監察官，即為因應不同領域處理個人資料之特性，所為之專精化安排。觀察我國目前所採行之分散式監管機制，同時有首長制及合議制機關者，而未來應參採何種制度，應可配合我國就欲採行單一或多個監督機關之體制，為進一步思考。

二、 個資特定目的外利用要件

(一) 英國部分

英國 DPA 2018 之立法規範模式不在於過度嚴格地緊縮特種資料禁止處理之原則，重點毋寧在確保各項個資保護基本原則之實現與衡平，尤其是透明性原則以及課責原則，二者能充分建立穩定社會信任基礎的原則。

另外，我國個資法欠缺的「利益權衡條款」以及未有對於「公共利益」之輪廓描述，亦為與英國重要之區別。

(二) 德國部分

相較於 GDPR 第 9 條對於特種個人資料所採「原則禁止，例外許可」之處理模式，德國個資法並未全面「原則禁止」特種個資之處理，而於德國個資法第 22 條明定處理特種個人資料之合法要件。而針對特

種個人資料之目的外利用，其要求應同時符合以下要件：

－一般個人資料目的外利用之要件，即分別規定於德國個資法第 23 條第 1 項（公務單位之目的外處理）及第 24 條第 1 項（非公務單位之目的外處理）中之要件；以及

－具備 GDPR 第 9 條第 2 項對於處理特種個人資料所定例外要件；或德國個資法第 22 條所定處理特種個人資料之要件及相應應採行之程序、技術。

與我國個資法第 6 條第 1 項但書就例外蒐集、處理、利用特種個人資料所為單獨規範之模式不同，德國個資法將「一般個人資料目的外處理之要件」以及「特種個人資料（目的內）處理之要件」，共同作為特種個人資料目的外處理之要件，在體例上大幅縮減重複規範之條文。但應強調者為，不論是目的內或目的外處理個人資料，對於「適當特定措施」（德國個資法第 22 條第 2 項）之採行，均屬不可或缺。

三、 去識別化相關規範

(一) 英國部分

去識別化之法律定義，歐盟各會員國認定大致相同，然還是有去識別化後之相對性與絕對性的議題尚待解決。在 GDPR 層面與 DPA 2018 之面向上，相關規範與實務均特別強調如欲判斷一個自然人是否可識別，則其判斷標準應考慮資料控管者或任何其他人通常自行決定可能使用的所有手段，以直接或間接識別自然人。

就「技術保護措施」言，為決定當事人是否可被識別，應考慮到所有可能合理使用之方法；而匿名化與假名化二者之區別標準在於判定何種結果才屬於可接受的資料再識別風險。假名化後，意欲回溯得到連結（re-link）而應用的個人資料，需頗耗費時間精力等成本，或部

分去識別化方法甚至難以回覆而辨識個人，而逸脫於可得識別個人的個人資料定義範疇之外，並以之作為個人資料保護之手段。在此必須理解，任何對去識別化資料之利用與再利用，仍然需要持續確認個資受侵害之可能性

就「組織性措施保護措施」言，則首應考慮相關的法規範和處理環境，並建立機構性的專責監管機關，並佐以 DPO 制度之落實。

(二) 德國部分

德國個資法一直以來，都將去識別化技術視為在維護當事人法益之適當且特定之措施中，所不可或缺者，德國法針對去識別化技術之運用，納入德國個資法第 22 條第 2 項所定「適當特定措施」中，並例示 10 款可能之措施。但此次修正將原先於舊法中有定義之「假名化（Pseudonymisierung）」刪除，直接適用 GDPR 之規範；而「匿名化」之要求，則得見於各別處理個資之要件中，例如：德國個資法第 27 條第 3 項針對基於科學或歷史研究目的以及統計目的處理特種個人資料，即有匿名化之要求。但於不同情況中，究竟應選擇何種去識別化措施，普遍仍認應依據 GDPR 第 35 條進行個資保護影響評估之結果決定之，故對於去識別化應達到之程度，包括方式之選擇及判斷之標準等，德國個資法中似選擇留白，給予個案依實際情況有彈性選擇之空間。另外，德國個資法第 22 條第 2 項要求控管者或受託處理者應考量技術之發展情形；採行之成本；處理之形式、範圍、狀態及目的；以及因處理而對當事人自由權利所招致風險之各種可能性與嚴重性，以決定應採行何種「適當特定措施」。德國個資法第 22 條第 2 項在體系上雖是針對特種個人資料之處理，但其亦被援用為處理其他個人資料情形之合法要件。

四、 特殊處理情形

(一) 英國部分

1. 個資保護與言論及資訊自由

臺灣雖然在學說與實務上普遍接受英國相關指引中包括個案中比例原則之權衡、關於同意之程序應特別注意、報導公眾人物之私下不正行止或因為其行止而特別受矚目的準公眾人物、特別注意處理個資之目的，以及衡平人性尊嚴與公共利益之問題等說明。然，目前臺灣似無相關指引或政策方向，如英國法制環境中指出的，個資保護所可能被調和，以及無法在此等衝突情狀下讓步的個資保護原則或規範。

2. 政府資料供接近使用與其個資保護

歐盟相關規範一再強調，並非被判定為個人資料或個人隱私事項即不得公開，而是必須判斷保護的法益之間彼此的衡平。又實務上，並無類似的操作階段區分，以確認政府資訊公開及個資保護之衡平環境。

3. 國家識別代碼與個資保護

事實上，並非所有國家均有此等制度，英國即為適例。這或許能在某些程度上給予我國關於身分證換發時的考量機會，甚至是從頭反省是否仍需要此等識別制度。

4. 僱傭關係與個資保護

我國勞動法規上,尚未有明確法令規範如英國僱傭實務準則一樣，從應徵直到退休一系列勞動者的個資保護說明，而是分別散落在個資法以及包括就業服務法、勞動基準法、職業安全衛生法及相關施行細則，以及相關機關的函釋當中。

在此需特別注意者，基於勞動者通常在職場上相對於資方係為弱勢,但(尤其是中小企業)資方有時也會有無力面對取巧勞方之可能，則如未來我國有個資獨立專責機關，在落實個資法時不妨借鏡英國之

經驗，採取針對不同需求者，分別給予不同的權利保障宣導。

5. 基於公益之檔案儲存目的、基於學術或歷史研究目的以及統計目的之處理

我國個資法雖然也有此等例外調和之規範，但卻未有明確地如同DPA 2018較細緻化之調和規範，將當事人權利類型於基於學術或歷史研究目的，及基於公益之檔案儲存目的之情況分別處理。

(二) 德國部分

德國個資法對於處理個人資料，各別規範其要件者，可分為以下三種情形：其一，係針對 GDPR 第九章中所定特殊處理之情況，訂定更細部之規範，包括：基於就業關係之目的處理資料（德國個資法第26條）、基於學術或歷史研究目的以及統計目的之處理（德國個資法第27條）、基於公益之檔案儲存目的之處理(德國個資法第28條)。其二，針對經濟活動中處理個人資料之行為，針對消費借貸之資料處理（德國個資法第30條）以及對於使用計分數值（Scoring-Werte）及支付能力查詢（德國個資法第 31 條），另行訂定規範，致力於經濟交易中保障消費者權益並確保市場公平競爭。其三，德國個資法第 4 條針對於公眾得出入之場所架設監視器之行為，定有一般性之規定，作為公務單位或非公務單位設置監視器時之法律依據。

由於德國個資法對於特殊處理情況，原則上係對 GDPR 所定處理要件為鬆綁，並大多因此伴隨著限縮當事人權利行使之效果，但亦可見要求控管者採行例如適當特定措施（德國個資法第26條第3項、第27條第1項、第28條第1項 ）、強化告知義務（德國個資法第4條第2項）、當事人同意有效性之確認（德國個資法第26條第2項）等，在追求個人資料合理利用與保護當事人權利間，求取平衡。但應強調者為，前述於德國個資法中所定特殊處理情形，均屬框架性規範，仍可透過特別法就細節為補充。

五、 自動化機器做成決定

(一) 英國部分

在關於自動化（包括人工智慧）做成治理不實訊息投放之決策上，例如新型態自動化訊息回覆機器人(bot, chatterbot)[298]等，本報告認為其治理基礎或許在一定程度上可參考歐盟之法規範與實際操作模式，其原因除前述個資保護為該操作模式之重要核心，而歐盟對個資保護之影響引領國際以外，更重要的原因在於在實務上具國際規模的大型社群媒體平台，尤其是在臺灣用戶最多的幾個平台如 Facebook、Google、Mozilla、Twitter 與 Microsoft，以及國際上大型貿易組織等均簽署「歐盟不實訊息實踐準則(EU Code of Practice on Disinformation)」，[299]並對歐盟提出實踐包含有自動化做成決策之作為具體措施。

英國 DPA 雖早在 1998 年版本即有相關規範，但是英國 2018 年 DPA 亦配合 GDPR 第 22 條規定，制定相應國內規範，改變 1998 年資料保護法原則上容許資料自動化決策之規定，而使當事人有權利發出通知，請求資料控管者不要使用其個人資料做出任何自動化決策；並要求資料控管者重新考慮通過自動化方式做出的決定。另方面，資料控管者新增責任包括:主動告知當事人有關剖析和自動化決策的資訊；進行此類處理時，需採取適當的防護措施；以及對當事人說明個人行使相關權利的程序。另外，其他特別限制則適用於特種個資和涉及兒童的自動化決策。

(二) 德國部分

---

[298] Bot 係指能夠透過聲音及文字與用戶進行對話的電腦程式，可以分為三種型態，分別為有預先腳本的預設腳本 bot、人工智慧 bot，以及混合真人的協助代理 bot。

[299] European Commission, *Roadmaps to Implement the Code of Practice on Disinformation*, Oct. 16, 2018, https://ec.europa.eu/digital-single-market/en/news/roadmaps-implement-code-practice-disinformation (last visited Jul. 31, 2019).

德國個資法第 37 條中，針對 GDPR 第 22 條第 2 項中「履約所必要（第 a 款）」以及「經當事人明確同意（第 c 款）」二種例外得為自動化決定之情形，首先將其適用範圍限縮於「依據保險契約提供給付」之範圍內，且須經當事人同意或該決定與適用對治療行為具拘束力之收費規定有關，且控管者已採行適當維護當事人權利之措施。另外，針對自動化決定之作成，德國個資法第 37 條第 2 項允許處理健康資料，但控管者於此必須相應採行德國個資法第 22 條第 2 項中所舉維護當事人法益之適當特定措施。此亦屬德國立法者依據 GDPR 第 9 條第 2 項第 g 款，對於健康資料之處理，於德國個資法中所制定之特別規範。

六、 當事人權利

(一) 英國部分

GDPR 第 23 條賦予會員國一定之調整空間，得以內國法限縮 GDPR 所規範當事人權利相關之適用要件。對此，英國 DPA 2018 於附件 2 第 3 部分與第 4 部分加以限縮權利之適用要件，即保護他人權利以及基於規範 GDPR 第 13 條及第 14 條之告知義務、第 15 條之近用權，並鬆綁前述三個條文對應在 GDPR 第 5 條第 1 項第 a 款至第 c 款之相關原則。

GDPR 關於兒童個資之特別保護要求，當然均在 DPA 2018 中落實規範。比較特別的是，DPA 2018 為此在第 123 條規範要求資訊委員必須加以準備「適合年齡設計準則(Age-appropriate design code)」。而第 123 條第 1 項規定即係此所指對於資訊委員之要求，需注意者，該準則要求之範圍仍僅限定在 ISS 內。而對該準則，DPA 2018 第 123 條第 2 款進一步賦予資訊委員修訂之權限，但仍須分別就兒童、父母、代表兒童權利者、兒童發展專家、商業團體代表等不同面向，與國務卿諮詢（第 123 條第 3 項）。如資訊委員認為需修正，則在準備上的考量點必須至少包括：兒童在不同的年齡層有不同需求之事實，以及英國就聯合國兒童權利公約所應負擔之責任。

對比我國，雖然我國在 2014 年 6 月 19 日也為實施聯合國 1989 年兒童權利公約，健全兒童及少年身心發展，落實保障及促進兒童及少年權利，制定了「兒童權利公約施行法」，但我國個資法與施行細則目前並未特別地如 GDPR 針對兒童個資保護作出特別規範。又，基於此處範圍僅限縮在 ISS，但我國卻無對應規範，因此未來如果個資法修法而意圖納入相關規範，或許可以借鏡英國相關之指引而指出相關適合年齡的設計標準，符合個資保護設計與預設(data protection by design and by default)之精神。

(二)　德國部分

相較於 GDPR 第 8 條針對兒童於 ISS 中作為當事人主體適格性所建立之認定標準，德國個資法就此並未有明文，故其將適用 GDPR 所定標準。但是否得以兒童之同意作為處理個人資料之合法要件，德國法在實務上仍多主張應與民法之行為能力切割觀察，強調應將重點置於兒童對提供個人資料行為所代表之法律上意義及效果，是否具有充分的理解與認知能力，於個案中為實質判斷。

針對當事人之權利，德國個資法第 32 條至第 37 條，即依據 GDPR 第 23 條賦予各會員國之權限，以內國法限縮 GDPR 所規定當事人權利之行使，包括：免除 GDPR 第 13 條及第 14 條關於直接或間接蒐集而為後續處理之告知義務（德國個資法第 32 條及第 33 條）；針對 GDPR 第 15 條近用權於德國個資法中所定特殊處理情形中，包括：基於科學或歷史研究目的以及統計目的之資料處理（德國個資法第 27 條）、基於公共利益之檔案儲存目的之資料處理（德國個資法第 28 條）以及德國個資法第 29 條針對負有保密義務情況下之當事人權利之主張，加以限制（德國個資法第 34 條）；限縮 GDPR 第 17 條第 1 項所定刪除之權利（德國個資法第 35 條第 1 項）；針對 GDPR 第 21 條賦予當事人之拒絕權，限縮其得主張之範圍（德國個資法第 36 條）。但對前述對於當事人權利行使之限制，德國個資法多輔以利益權衡條款，要求於個案

中就當事人權利與處理個人資料之利益間為實質判斷，以求衡平。

第二節　我國個資保護課題與建議

關於我國個資保護相關法制現狀，大致上相對完整的立法與相關施行歷史介紹與分析在近年的各式研究報告、期刊論文，以及政府出版當中，均可尋得[300]。而關於我國個資保護法制應進行相當程度之改革與變動之建議，亦不難發見。尤其，為因應 GDPR 之施行以及 GDPR 對原有資料保護指令之修改與強化，且我國在政策上希冀獲得歐盟對此的適足性認定，更顯我國個資法有修改之必要性。

以下僅就本報告發現之課題，以及本報告前部分之歐盟會員國落實 GDPR 經驗，提出遭遇並需積極面對的課題。

一、 強化監督機制之必要性：沒有一個獨立專責監管機關，則幾乎完全無法具體面對數位時代下資料治理的根本問題，以及 GDPR 帶來的個資保護新制度挑戰

本報告在前述關於中央與地方監管機關部分，即說明了一個獨立專責監管機關相關之職權與地位。在此雖然幾乎大部分臺灣目前的文獻均在一定程度上支持並強調臺灣應有個資保護的獨立專責機關，以取代目前分散式的管理，但本報告仍援引英國現任資訊委員在針對 DPA 2018 之監管行動政策(Regulatory Action Policy)前言所提到的幾段話，來具體說明究竟一個專責監管機關能解決目前臺灣個資法制的困境到什麼程度[301]：

我既是教育者，同時也是監察使，在大多數情況下，這就

[300] 例如：劉定基，2020 年 1 月，The Past, Present, and Future of the Right to Information Privacy: A Comparative Law Perspective，收於：司法院大法官書記處編輯，釋憲七十週年國際學術研討會論文集，司法院，頁 313-338。

[301] ICO, Regulatory Action Policy, https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf, 3.

足夠了。但是有時候，教育的胡蘿蔔沒有引起人們的注意，監管者便必須使用他們的棍子–因此，我也有能力採取執法行動，並在有需要時採取制裁措施。…

…我相信這項監管行動政策表明ICO是既是個人資訊權的強有力捍衛者，又是組織尋求以負責任和安全的方式使用資料的推動者。那些受ICO監管行動約束的人應該毫無疑問地認為，我們將以透明、一致和相稱的方式來追究法律的失能之處。

最終，我的辦公室的存在是為了維護數位時代個人的資訊權。…

除了透過設置監督機關由外而內就個人資料保護之落實情形進行監管外，個人資料之控管者如何由內而外落實法遵，亦為重要課題。相對應 GDPR 在監督機制中所設置之 DPO 職務，我國個資法雖亦要求「公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏」（個資法第 18 條）以及「非公務機關保有個人資料檔案者，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」（個資法第 27 條），而其中之「採行適當之安全措施」即包括「配置管理之人員及相當資源」（個資法施行細則第 12 條第 2 項第 1 款）。但如何善用該「專人」或「管理人員」，使其實質參與並影響個人資料保護之內控工作及發揮與監督機關間順暢之溝通與對話功能，此應屬監督機制中可再予以強化者。

二、 個資特定目的外利用要件

在 GDPR 之架構下，英國及德國針對個資之特定目的外利用，均有鬆綁之趨勢，藉以達成個資之合理利用。英國 DPA 2018 重視同步強化透明性原則及課責原則，除藉以保障當事人權利外，亦達成社會信任基礎之建立。德國個資法在目的外利用規範之特殊性，則見於對特

種個資目的外利用之要件，其要求除應符合一般個資目的外利用要件外，尚須具備 GDPR 或德國個資法對於處理特種個資所定要件。另外，亦透過導入德國個資法對於處理特種個資所定要件，對於目的外利用之情形，強調採行「適當特定措施」之重要性。

相較之下，我國個資法在規範特定目的外利用之要件中，欠缺為兼顧個資合理利用及個資保護之「利益權衡條款」，尤其是當特定目的外利用之要件，係由不確定法律概念所構成時，如：公共安全、公共利益等，仍應讓公務機關及非公務機關於個案中就所欲維護之具體利益與當事人權利保護，享有一定程度之判斷餘地；而對於「公共利益」之範圍界定，也未有一定程度之界定或例示，甚至如英國 DPA 2018 在附件詳加區分類型與定義。

我國個資法並未將「適當安全維護措施」作為就一般個資及特種個資進行目的外利用之要件之一，而僅係課予公務機關與非公務機關一般性之安全維護義務，應可考量於目的外利用時，適度提升安全維護措施強度之要求，作為衡平個資合理利用及當事人權利保障之方式之一。而對於德國個資法規範特種個資目的外利用之特殊體例，雖得收避免重複規範，使法條規範更加精簡之效，但考量此種法律適用結果並非「一望即知」，我國若欲參採此種模式，即不宜僅透過解釋，而應於條文要件中予以明確規定，較為穩妥。

三、 公務機關、非公務機關與公共利益的難解糾葛

首先，在 GDPR 中原則上並無區分，亦即公務機關與非公務機關一體適用各項基本原則。為此，公務機關亦體認應當付出公務成本。但在我國個資法目前仍為雙軌制，因此公務與非公務機關適用之規則，尤其是個資保護與其他基本權利相互競合之的衡平調和有其差異，而

我國個資法卻無利益衡量之條款[302]，故在實際操作上可能發生困境。

這項差異尤其可能會在個資法第 15 條與 19 條在比較時，就其中第 19 條第 1 項第 6 款「為增進公共利益所必要」時，發生更大的問題，因為在此遇上了對於「公共利益」這個不確定法律概念加乘「必要」的比例原則操作衡平概念的困難。

就此對照 GDPR，GDPR 雖為歐盟法律位階上的「規則」層級，但是授權會員國可以就「公共利益」與國家安全事項對公務機關有豁免規定，惟需符合比例原則，且該等公共利益需達到特定且重要之標準（例如：洗錢防制）。而在本報告前述關於 DPA 2018 附件中對公共利益之較具體之長篇規範，臺灣的個資法則顯得相對地模糊。

四、 個資蒐集、處理及利用之階段區分造成運作判斷困難

關於 processing 之定義在 GDPR 第 4 條第 2 款中，指的是所有關於個人資料之呈現或是對資料集之一切自動化或非自動化作為，包含蒐集、紀錄、組織、結構化、儲存、接收、轉換、檢索、詢問、利用、揭露、傳播、得運用於演算（法）中、合併、限制、抹除、或是破壞等行為，均是所謂 processing 之範圍。換句話說，此處之 processing 內涵上兼及我國個資法定義上之「蒐集」、「處理」以及「利用」之所有階段。在個資利用限制原則所觀察之階段討論個資之再次蒐集、處理與利用時，無論是否合於目的，或是目的外使用時是否兼容於蒐集個資時之特定目的，其所指乃係對於當事人蒐集個資後的所有之關於個資之一切作為[303]– 這與我國個資法第 16 條及第 20 條對目的外利用是否兼容於蒐集時特定目的之檢驗，僅限於「利用」之階段，有所不同。

302 即類似「為資料控管者或第三人正當利益所必要。但當事人對該資料之保護具有更重要利益者，不在此限」之規範。但學者也認為該等條款不應在公務機關適用。參：范姜真媺、劉定基、李寧修，「法務部『歐盟及日本個人資料保護立法最新發展之分析報告』委託研究案成果報告」（2016 年），頁 199。

303 Article 29 Data Protection Working Party (2013). “Opinion 03/2013 on Purpose Limitation.” (00569/13/EN WP 203, 2013). http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, 21.

而恰恰是這個不同，在我國實務上發生之訴訟案件，引起討論。例如，公務機關之「目的外之處理」並非第 16 條之規範範圍（該條僅規範利用之行為）。例如，公務機關對於個人資料資料庫之整併或是（編輯、複製）與內部傳送係為個資法上定義之「處理」，此時因非為第 16 條範圍，則此際目的外之處理行為，即生管制上之疑義。

然而，在巨量資料之實際技術考量下，「再利用」之概念至少應當被界定為在合於原特定蒐集目的下之主要利用（primary use），或合於包含法定義務等例外情狀以外之其他對於個人資料之利用。巨量資料技術對於個資之「再利用」，事實上必須包含對於資料庫內個人資料之所有以演算法而為之自動化運作行為態樣，然而這些行為態樣如依照我國前述討論之現行個資法規範，則不盡然都落在「利用」之定義範圍，而可能落在「處理」之定義中，並進而發生法規適用之問題。關於個資的「再利用」就邏輯上言，可進一步地區分為三種不同情狀，[304] 最大的問題癥結為個人資料在蒐集階段之同意，因為同意前的告知事項基於資料集不斷地進行重組而牽涉不同個資，告知之內容將因為愈趨複雜且不斷地膨脹，因此種種因素實務上越來越難使得當事人真的閱讀完並理解該告知內容後而為同意之意思表示[305]。

五、 產業使用個人資料所遭遇的最常見難題：去識別化在我國個資法與相關法制架構中，意義混淆不明

歐盟在其「邁向一個共同的歐洲資料場域(Towards a common European data space)」通訊中[306]，指出歐盟在資料發展相關產業政策上

---

[304] 此三種情狀為：
•情狀 1：該當事人 A 並不知悉其個人資料已被他人 B(通常為個資控管者，但部分情狀亦可能僅為個資儲存或利用人)處理與利用;
•情狀 2：B 違反 A 之自由意志而對於 A 之個資加以處理與利用;以及
•情狀 3：A 表明放棄個資保護諸權利所保障之利益。
關於各情狀之討論，詳參：翁逸泓，2018 年 3 月，科技人權－全民電子通訊監察與個人資料保護，臺灣民主季刊，第 15 卷第 1 期，頁 23-24。

[305] 前揭註，頁 22-30。

[306] European Commission, Towards a common European data space, Brussels, 25.4.2018,

的主軸為：

1. 透明度：相關的契約協議應以透明且易於理解的方式確定（i）將有權近用產品或服務生成的資料的個人或實體，此類資料的類型以及詳細程度；(ii）使用此類資料的目的。
2. 共享價值創造：相關的契約協議應認識到，當資料作為使用產品或服務的副產品而產生時，事實上是有多個參與者為創建資料做出貢獻。
3. 尊重彼此的商業利益：相關的契約協議應解決保護資料所有者和資料使用者的商業利益和秘密的需求。
4. 確保不失真的競爭：相關的契約協議應滿足在交換商業敏感資料時確保不失真的競爭的需求。
5. 資料之鎖定(lock-in)予以最小化：提供以產品或服務之副產品形式生成資料的公司，應盡可能允許並啟用資料可攜性。其還應考慮在可能的情況下根據其經營的市場特點,提供相同的產品或服務，而無需或僅提供有限的資料傳輸，以及包含此類資料傳輸的產品或服務。

而所有的主軸事實上無論是企業對企業(business-to-business, B2B)或是政府對企業(business-to-government, B2G)的資料傳輸分享類型，都圍繞著個資的再利用。但是這個再利用許多時候在臺灣的實務上，無論是業者或是政府都會遇到關於「去識別化」究竟是什麼以及應該要做到何種程度的障礙。

我國個資法中散見之「適當安全維護措施」、「安全維護事項」以及「適當之安全措施」等要件，考量其屬處理個人資料之重要配套機制，或許可考慮德國模式，採取集中規範的方式，以我國個資法施行細則第 12 條第 2 項為本，進一步參考 GDPR 或他國對於安全維護措施

COM(2018) 232 final, https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-232-F1-EN-MAIN-PART-1.PDF, 10.

之普遍要求，予以強化，除可有效提升法律明確性，亦可免除於不同條文間重複規範之情況。然而，於各別個案終究竟應選用何種「去識別化措施」，恐怕仍不能忽略採行個資保護影響評估之重要性，並將當代技術發展情形，採行之成本，處理之形式、範圍、狀態及目的以及因此對當事人權利可能導致之風險一併為妥適考量。但如同德國個資法，針對特別處理情況，仍得於此基礎上，直接由立法者權衡後，提高彈性或降低安全維護措施之等級，例如：要求採行匿名化或強化刪除義務。

六、 個資法對當事人之權利保障並未跟上數位/AI 時代發展需求：機器自動化做成決策的法規真空

我國之個資法雖有將個人資料檔案定義為「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」之類似於自動化機器之文字敘述[307]，卻並無任何個資法上之獨立法條對於該等自動化機器做成之決定與評價作出明文規範、保護乃至於例外情狀之判準，更遑論與本報告前述 GDPR 關於自動化做成決策之拒絕權與審查/解釋權相銜接。本報告作者之一對此曾提出，「在法規範接近真空之狀態下，政府邇近大力推行之科學技術發展重點領域如關於電子健康資料人工智慧之研發與加值應用等，又該如何真正地面對來自於個資法之潛在『挑戰』呢？」[308]

我國科技部事實上也在 2019 年底發表公布了「人工智慧科研發展指引」，[309]但該文件卻僅指出概略性之基礎原則，例如在個資保護面向上，僅有[310]：

---

[307] 個資法第 2 條第 2 款參照。

[308] 翁逸泓，2019 年 2 月，開放全民電子健康資料加值應用之個資保護問題－以英國經驗為例，月旦法學雜誌，第 285 期，頁 170。

[309] 科技部，人工智慧科研發展指引，https://www.most.gov.tw/most/attachments/53491881-eb0d-443f-9169-1f434f7d33c7。

[310] 前揭註，頁 2-3。

個人資料隱私侵害的預防，必須建立有效的資料治理，在 AI 研發與應用上，AI 科研人員應致力注意個人資料蒐集、處理及利用符合相關法令規範，以保障人性尊嚴與基本人權，並針對 AI 系統內部之個人資料架構有適當的管理措施，以維護當事人權益。

上開文字，本報告認為，於細部規範上若我國未來能有一個個資保護獨立專責機關，則其不妨參考英國 DPA 2018 之落實或另為詳細說明。

又，此處關於自動化決策之規範，不但牽連有本報告之個資保護關於當事人權利乃至資料控管者義務之規範，事實上亦有關於政府近來推動開放政府資料，甚至進一步推動商業、產業化運用政府資料時，導入 AI 或其他自動化決策方式，除在公平交易與智慧財產法規範上之財產分配規範外，仍須對以個資作為驅動來源之相關產業，有相關配套之個資保護法制規範。

七、 通訊傳播、生醫健康研究等個別產業面向、勞動保護與個資保護之交錯問題，或許應有專門規範

我國個資法雖未採 GDPR 或德國個資法將所謂「特殊處理情況」納入規範之體例，但就不同領域中確實可得見特別法之規定。但由於特別法多非以保護個人資料為其立法目的，故對於個人資料法制中相當重要者，包括基本原則、當事人權利、安全維護措施等，大多未有相關規定，或規範地相當簡略，故針對特殊處理情形，若能於個資法中為框架性規定，對於規範之一致性及對個人資料保護之完整性，應當有所助益。

在本報告關於 GDPR 與其他基本權利保障事項相調和的特殊處理情形中，事實上可以觀察到的是即便是「嚴格」如 GDPR，也會給予會員國國內法一定的評斷餘地，作為立法之形成空間，以符合相應之國內在地法制現況與文化。即便如同英國對於健康面向之研究與個資

保護無另外專門之立法，而仍回歸到 DPA 2018 與 GDPR，但是仍有相關之準則，例如英國數位全民健康服務與醫學研究委員會共同制定之「由健保資料庫取得資料供健康研究之指引」，英國之健保資料庫對於資料之應用、治理與釋出分享模式具相當詳細之說明。而德國對於健康資料之處理，亦未定有專法，但其規範係散見於聯邦及各邦之法律中，例如：德國個資法第 27 條對於基於研究或統計目的處理個人資料之規定；德國社會法典對於社會資料、法定醫療保險及法定照護保險相關資料之處理；器官移植法等。另外，聯邦經濟及能源部（Bundesministerium für Wirtschaft und Energie）亦針對非公務單位處理健康資料，特別是目的外處理之情形，創造經濟價值，提供相關指導。

至若因應數位匯流時代之法律規範，基於我國已有國家通訊傳播委員會(NCC)之獨立專責機關，地位對應英國之通訊辦公室(Office of Communications, Ofcom)。然，「數位通訊傳播法」以及「電信法」修法之相關草案雖已送入行政院會，但等待多時仍未見具體審議時間。而 NCC 計畫草擬之 OTT-TV 對應法規「網際網路視聽服務法」也仍未見具體草案輪廓，則對應個資保護交錯之相關指引，當然也難尋蹤跡。基此，個資法未來修正時如仍以個資保護之普通法為定位，則在須靈活變通的數位匯流時代通訊傳播法中是否有針對特定類型資料或者特定目的利用，仍得解釋為有增訂特別規定的空間。

最後，關於勞動保護的部分，目前實務上雇主保有許多勞工的個資，以我國個資法是否足以保障勞工的權益？雖然比較法上例如英國之 DPA 2018 也無體系性關於勞動隱私之規範或特別規範，但仍有整合性之指引。反觀目前我國仍無整合性之勞動上個資實務規範或指引，僅在個別面向上有相關散落之函釋。

以勞工健康檢查為例，依據勞動部職業衛生安全署解釋，依據「職業安全衛生法」(下稱職安法)第 20 條規定，勞工健康檢查係法律規定雇主應為勞工辦理之項目，其目的係為選工、配工、職業病預防與職

場健康管理。故該署認為事業單位對其所屬勞工依「勞工健康保護規則」(下稱本規則)所定期限及項目之檢查結果，得依法進行紀錄之保存、處理及利用，尚無需另經勞工書面同意，惟不得逾越前開特定目的範圍，且須依本規則第 21 條第 3 項之規定保障勞工隱私權，以符個資法之規定。而關於應採行之安全衛生措施，也認為基於職業安全衛生設施規則第 324 條之 1 至第 324 條之 3，而合於個資法第 19 條及第 20 條法律明文之規定。[311]

然而同一份解釋中也說明似乎勞工得拒絕提供該項健康檢查資料：「尊重個人隱私及瞭解勞工不願意接受之原因，再透過勞資協商解決對策；若該勞工仍堅持拒絕，建議留存相關執行紀錄。」，然隨後又另基於實務上常有因健康檢查後續應採取相關健康管理措施而衍生勞資爭議，該署認為職安法施行細則第 41 條已將健康指導及管理措施，增列為安全衛生工作守則內容之一，依職安法第 34 條之規定，勞工對於該守則應切實遵行，建議事業單位亦可將相關之健康管理措施納入該守則規範。

據此，可見實務上即便主管機關之函釋，亦仍有一定之模糊性存在，於勞工隱私權與健康管理措施意欲保障之資方選工、配工、職業病預防與職場健康管理發生競合時，究竟應如何衡平似仍有猶豫。可能的解決之道或許仿照英國由個資專責主管機關發布整合性指引。就目前而言，則不妨借鏡參考日本，由勞動部訂定相關指引，整合勞工個資保護的問題。

八、 當事人權利之類型及其行使之界限

我國個資法第 3 條所規範之當事人權利，包括查詢或請求閱覽；請求製給複製本；請求補充或更正；請求停止蒐集、處理及利用以及

311 勞動部職業安全衛生署，常見問答，https://www.osha.gov.tw/1106/1196/10101/10112/10115/17019/。

請求刪除，且該等權利不得預先拋棄或以特約限制之。由於對「當事人」並未有資格之限制，故針對兒童於個資法中作為當事人之法律上定位，包括同意之作成、告知義務之履行以及當事人權利之主張，應是在界定「兒童」之同時，不應忽略之面向。

另外，對於當事人權利行使之限制，我國個資法之規定較為簡略，僅於第 10 條以及第 11 條第 3 項但書中，分別規定對於查詢、閱覽及製給複製本權利以及對於刪除、停止處理及利用請求權主張之限制。但現行法就當事人權利之主張，是否有其他限制之可能？具體之限制要件究竟為何？以及是否應輔以何種配套？恐怕皆不甚清晰。但實務上曾發生當事人主張停止蒐集、處理、利用之「退出權」[312]，或是要求刪除特定資訊之「被遺忘權」的實例[313]，某種程度皆反應出我國個資法對於當事人權利之規範，應有再行檢視之必要。另外，考量當事人權利之保障，應屬個人資料保護法制之核心內涵，除應要求控管者於處理個人資料時，致力於當事人權利保障之落實外，若欲限制當事人權利之行使，在法律保留及法律明確性之要求，恐亦不容忽視。

[312] 該案涉及全民健保資料之利用問題，歷經臺北高等行政法院 102 年度訴字第 36 號判決、最高行政法院 103 年度判字第 600 號判決、臺北高等行政法院 103 年度訴更一字第 120 號判決及最高行政法院 106 年度判字第 54 號判決定讞。其中原告即主張縱使個資法第 16 條列舉可不經當事人書面同意而為目的外利用之各款事由，但事前無須經當事人書面同意，並不等同其享有事後控制權，當事人仍得基於資訊自主權，依個資法第 3 條第 4 款之規定，「事後」請求停止原蒐集目的外之再利用。

[313] 該案原告主張依據歐洲法院 103 年 5 月之判決，被告身為搜尋引擎業者，須保障用戶個資，民眾有權要求被告刪除與「過去行為」或「批評」相關之「不當個人資訊」的「搜尋連結」，以維護民眾之「隱私及名譽」，並保障其應有之「被遺忘權」。相關判決請參考臺北地方法院 103 年度訴字第 2976 號判決、臺灣高等法院 104 年度上字第 389 號判決、臺北地方法院 104 年度訴更一字第 31 號判決及臺灣高等法院 106 年度上字第 1160 號判決。

第五章　結論與建議

本報告之目的係針對歐盟會員國如何落實 GDPR 之情形加以觀察並分析，對此本報告分別對德國個資法與英國 DPA 2018 之內容及二國各自落實 GDPR 之實際情形提出觀察，且另就擇定之重要議題分析英國、德國與我國個資法之異同。這幾個議題分別是監管機關之中央與地方權限、個資特定目的外利用之要件、去識別化之要件、程序、認定方式等規定、特殊處理情形(GDPR 第 9 章)、自動化機器做成之決策，以及當事人權利之議題相關的法律制定與政策落實。就此，本報告以下分別提出英、德二國對 GDPR 落實之共同點，並提出可能作為我國參考之借鏡與建議。

一、 兩國共同之處

就比較德國與英國落實 GDPR 之法律制度與政策實踐而言，具體來看二者因為內國法制度不同的關係而有所差異，但事實上也有共同之處。

首先，在監管機關方面，兩國咸認該等機關須具有獨立性，且因為考量個資保護與政府資訊公開之間法益競合機會頻繁而須進行權衡，因此均將此二職權交由同一機關執掌。此外該等機關之數量無論是否單一，均須「專責」個資保護事務。

在特種個資之處理方面，與一般大眾對 GDPR 係「全世界最嚴格的個資法」觀念略有差異，事實上在兩國實際落實的經驗下可以發現雖然該「規則」具有相當高的拘束力，但事實上 GDPR 本身有許多使會員國調和其內國法制與豁免部分，於緊縮處理之規範容許例外存在，似有放寬之跡象與空間。

在去識別化方面，雖然有意見認為我國目前對去識別化的定義不清楚，但若從德國與英國的實踐來看，再進一步明確化「去識別」的

定義確實是有難度的事情，因此我國未來修法是否要訂定去識別化的規定，或許可以參考這兩個國家及其他國家(例如日本)之作法。

至於特殊處理之情形、自動化處理與做成決策以及當事人權利之面向，也同樣地因為 GDPR 有使會員國依據內國法律架構與實際情況而調和之空間（例如：在例外允許個資處理之條件出現「依照會員國法律」之規範），因此可見到處理個資條件之鬆綁，並伴隨限縮當事人權利行使之結果，以及對於資料控管者為一定保護個資之措施要求。再者，此部分也都多有框架性規範，並配合特別法或指引作為補充。須注意者，無論是德國或是英國之規範對於此，有關於基本個資保障原則及對當事人權利保護之要件，實務上兩國最常出現之關於自動化做成決策例外經當事人同意得處理個資例子也都為保險契約，但是仍有採行適當維護當事人權利措施之條件限制。

二、 對我國的建議

本報告必須指出，許多討論在關注 GDPR 並加以分析時，經常忽略了所謂的 G，指的正是「一般性(general)」，也因此在歐盟層級的資料保護法體系上，除了 GDPR 以外，尚有包括「法律執行指令(Law Enforcement Directive)」、「電子通訊隱私指令(2002/58/EC, ePrivacy Directive)」、「資料留存指令(Data Retention Directive)」，以及研議中的「電子通訊隱私規則 ePrivacy Regulation（草案）」等特別規定，層層保護個人資料之權利。換言之，我國在法制上如要完善個資保護法制，甚至企圖實現良好的資訊治理，實有必要將相關特別法加以完備。

復次，一個獨立專責且能量充足的監管機關，是推動個資保護法制的必要機構性之保護架構。目前分散式的監管方式，已然造成許多新興數位科技發展實務爭議在監管機關找尋與確認上，屢生爭端。

而本報告在比較分析 GDPR 於歐盟會員國法制與實務上究應如何運作上，認為最基本的關鍵在於本報告所分析的所有重要爭點，都需

要仰賴這個專責機關依照所被賦予的職權：教育宣導、法令解釋、監督管理、執法制裁等具有能量的行政作為，來加以實現個資法制上對於當事人權利之保護，以及對於資料控管者義務之監督。

從而，對於我國監管機制之建立，首先建議呼應國際趨勢，設立獨立機關外，應使其專門負責個人資料保護之監管業務，而不宜同時作為「目的事業主管機關」，而減弱其獨立性。其次，由於「個人資料保護」並未列舉為地方自治事項，且具有全國一致性，應屬中央權限，而應設立單一（由中央主責，搭配各機關之資料保護監察官）或多個（中央、委辦地方）監督機關，應為接續須思考者，若欲建置多個監督機關，則監督機關間，如何確保有開放之溝通平台，共同合作，維護一致之個人資料保護標準，即屬採行非單一監督機關必須面對之重要課題；若係規劃設置單一監督機關，雖可收事權集中之效，但必須考量其是否有充足之量能足以因應，以及是否有因應不同領域之特殊性、處理之個人資料類型及方式、規模之相異，於機關內部再行妥適專業分工，故於此種情況，機關之體制即建議以採行合議制較為適當。

針對去識別化之規範，建議可參考德國個資法採取集中規範的方式，以我國個資法施行細則第 12 條第 2 項為本，進一步參考 GDPR 或他國對於安全維護措施之普遍要求，予以強化，訂定類似德國個資法第 22 條第 2 項就「適當特定措施」之一般性規定，除避免重複規範外，亦可讓控管者就其可能得採行措施之選項，有較高之預見可能性。而在特殊處理情況下，仍得於此基礎上，彈性調整安全維護措施之等級及類型。

我國個資法雖未就「特殊處理情況」予以明定，但就不同領域中確實可得見特別法之相關規定。觀察臺灣現況，由於個別法律多非以保護個人資料為其立法目的，故對於個人資料法制中相當重要者，包括基本原則、當事人權利、安全維護措施等，大多未有相關規定，或規範地相當簡略，甚至個別法律會規定「依個人資料保護法規定辦理」，

而回歸適用個資法；換言之，在我國法制實務上當其他法規利用到個資且要訂定個資蒐集、處理、利用辦法時，多會按照個資法規定處理。

故針對特殊處理情形，若能於個資法中為框架性規定，對於規範之一致性及對個人資料保護之完整性，應當有所助益。不過，在現階段未有個資保護專責監管機關之情形下，不妨維持由各目的事業主管機關訂定相關指引，以儘速整合各領域相關個資保護之問題。另方面，在個資保護與其他特殊權利類型較可能發生競合之領域，如通訊傳播、生醫健康研究應用、勞動保障等領域，則因其特殊性，應由各機關負責針對各個不同的法規進行規範或修正並執行。在此則必須考量如該等規範係由個別領域之主管機關制訂與執行，則倘若未來如有個資專責監管機關時，該二個（或以上）機關間權限相互衝突時應如何處理？

本報告認為，如在個別領域就個資保護範圍競合時，應由個資保護主管機關就此部分表示意見，並且尊重其意見。首先，各部會就個資保護事務未必均能掌握，而個資專責監管機關所能涵括之權限範圍，就英國與德國而言，本來就遍及各領域。再者，以前述英國關於政府資訊公開及個資保護發生競合為例，在檢驗之流程上如果所涉及之個人資料主體即為該申請政府資訊公開案件之當事人，則應循 GDPR 或英國 DPA 2018 之個資近用權請求，而非與之競合的政府資訊公開規範。

對於當事人權利之類型及其限制，我國個資法之規定較為簡要，權利之內涵，雖可透過解釋予以強化，然若欲限制當事人權利之行使，其實質與形式正當性即須受檢驗，故應以法律明確規範限制之要件，較為妥適。另外，觀察德國個資法於 GDPR 外，對於當事人權利進一步加諸之限制，其大多會輔以利益權衡條款以及相關配套，例如：書面記錄之要求、限制控管者之處理，應具參考價值。

此外，缺乏利益衡量之條款，也使得僵化而機械的文義解釋操作，

令社會大眾尤其是產業界產生對於個資法制之恐懼，擔心個資保護之落實會限制數位科技之應用，而紛紛希望以去識別化之方式脫離個資法範圍，又或期待創設各種例外豁免（特種）個資保護之規範，甚任意依照主觀心證解釋所謂「公共利益」之範圍與內涵。

最後，在追求至少跟得上 GDPR 腳步而落實相關法制的同時，或許面對我國數位經濟發展政策的渴望，在個資保護法制上對包括人工智慧（機器自動化）決策、通訊傳播與健康研究應用等不同領域上，各目的事業主管機關於法制上可以考慮「超前部署」，以其作為我國資訊治理政策的起點。

附錄一 德國聯邦個人資料保護法（2019 年 11 月 20 日修正）部分條文翻譯

第 2 條 定義

（1）聯邦之公務單位係指由聯邦、聯邦直接設置之公法社團、依據公法設置之公營造物與財團以及其所屬不論法律形式之團體，其所屬之行政機關、司法行政機關以及其他依據公法組織之機構。

（2）邦之公務單位係指邦、鄉鎮、鄉鎮協會或其他隸屬於邦由其監督之公法人以及其所屬不論法律形式之團體，其所屬之行政機關、司法行政機關以及其他依據公法組織之機構。

（3）由聯邦及邦之公務單位依據私法所設立之團體符合以下情形之一者，其擔負公行政任務者，不論其中非公務單位之參與程度，均視為聯邦之公務單位：

1. 其行使職權之範圍跨越單一邦，或
2. 聯邦具有絕對多數之持份或表決權。

其餘情形則將其視為邦之公務單位。

（4）非公務單位係指不屬第 1 項至第 3 項所定範圍內之自然人及依據私法設立之法人、公司及其他人合組織。若非公務單位執行公行政之高權任務時，則於該範圍內視為本法所稱公務單位。

（5）聯邦公務單位於作為公法企業參與市場競爭時，視為本法所稱非公務單位。邦公務單位於作為公法企業參與市場競爭，執行聯邦法以及其未透過邦法規範個資保護時，亦視為本法所稱非公務單位。

第 4 條 公眾得出入之場所之錄影監視

(1) 以電子設備監視公眾得出入之場所（錄影監視），僅得於下列情形為之，當：

1. 公務單位為履行任務，
2. 為維護家主權，或
3. 基於具體確定之目的保護正當利益所必要

且未有事由足認當事人值得保護之利益應為優先時。錄影監視使用於

1. 公眾所得近用之幅員廣大設施，特別是如運動場、集會或娛樂場所，購物中心或停車場，或
2. 交通工具及公眾所得近用之幅員廣大之公共火車、船舶及巴士站，

對於停留於上述地點之人的生命、健康及自由之保護，屬特別重要之利益。

(2) 應以適當之方式，儘早使人知悉監視之情況及控管者之姓名及聯絡資料。

(3) 儲存或使用依據第 1 項所蒐集之資料，限於達成蒐集目的所必要，且未有事由足認當事人值得保護之利益應為優先時，方得為之。第 1 項第 2 句準用之。基於其他目的再為處理時，僅以防止國家或公共安全之危害或追訴犯罪所必要者為限。

(4) 錄影監視所蒐集之資料與特定人比對者，其處理應依 GDPR 第 13 條及第 14 條告知該當事人。第 32 條準用之。

(5) 該資料若對達成目的已無必要，或繼續儲存違反當事人值得保護之利益時，應立即刪除之。

第 5 條 任命

（1）公務單位任命個資保護長。對於第 2 條第 5 項所稱參與市場競爭之公務單位，亦適用之。

（2）多個公務單位得考量其組織架構及規模任命共同之個資保護長。

（3）個資保護長之任命應依據其職業資格，特別是其於個人資料保護法制及實務領域之專業智識，以及依據其履行第 7 條所定任務之能力為之。

（4）個資保護長得為受雇於公務單位之人或依據職務給付契約（Dienstleistungsvertrag）履行其任務。

（5）公務單位公布個資保護長之聯絡資料並告知聯邦個人資料保護暨資訊公開監察官。

第 7 條 任務

（1）個資保護長於 GDPR 所定任務外，至少應負以下任務：

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

（2）個資保護長得承接其他任務或負擔其他義務。公務單位應確保其任務及義務未導致利益衝突。

（3）個資保護長相應承擔履行其任務時，於處理過程中所生之風險，就此其注意處理之形式、範圍、狀況及目的。

第 9 條 職權

（1）聯邦個人資料保護暨資訊自由監察官專責聯邦所屬公務單位之個人資料保護監管，其亦包括參與市場競爭之公營事業。本章之規定亦適用於雖非公務單位，但其由聯邦持股佔多數或掌握多數決策權，且其委託人屬聯邦公務單位之處理者。

（2）聯邦個人資料保護監察官不負責監督聯邦法院基於其司法職權處理個人資料之行為。

第 10 條 獨立

（1）聯邦個人資料保護暨資訊自由監察官以完全獨立之形式履行其任務及行使其職權。其不受到來自外界之直接或間接之影響，且無須請示或服從指令。

（2）聯邦個人資料保護暨資訊自由監察官僅於不影響獨立性之範圍內，就經費稽核受聯邦審計部之監督。

第 11 條 任命及任期

（1）聯邦個人資料保護暨資訊自由監察官由聯邦政府提名，經聯邦議會（Bundestag）不經討論經法定成員過半數同意選出。選出者由聯邦總統任命之。聯邦監察官於選任時應年滿 35 歲。其應具備履行任務及行使職權所必要之資格、經驗及專業知識，特別是於個人資料保護領域。其應透過相關任職經驗具有對個人資料保護法制之掌握且具備擔任法官或是更高等級行政職務之資格。

（2）.....

（3）聯邦監察官之任期 5 年。得連任 1 次。

第 12 條 職務關係

（1）聯邦監察官依據本法與聯邦間屬公法上職務關係。

（2）.....

第 22 條 特種個人資料之處理

（1）處理 GDPR 第 9 條第 1 項所稱特種個人資料，排除 GDPR 第 9 條第 1 項，應屬合法

1. 當其係由公務單位及非公務單位處理，

a) 為行使自社會安全權利及社會保護所由生之權利並承擔因此產生之相關義務所必要，

b) 基於健康照護之目的、為判斷勞動者之工作能力、為醫學上之診斷、健康或社會領域之照護或處置、為健康或社會領域系統及服務之管理或基於當事人與健康職業成員之合約所必要，且該個人資料係由醫護人員或具有相應保密義務之人員為處理，或於其監督下為處理，

c) 基於公共健康領域中公共利益之理由，如防護受到重大跨境之健康危害或維護較高品質及安全標準之健康照護、藥品及醫藥器材所必要；補充第 2 項所稱措施，於此應特別關注職業上及刑法上對於維護保密義務要求之遵守，或

d) 基於重大公共法益而有急迫必要，

2. 當其係由公務單位處理，

a) 為防止對公共安全之重大危險所必要，

b) 為防止對於公共利益之重大不利益或為維護公共利益之重大利益而有急迫必要，或

c) 基於軍事防禦或為履行聯邦公法單位之跨國家或國際間義務之理由，於危機處理、衝突預防或人道措施之領域有其必要，

且在第 2 款所稱資料處理之情形中，控管者之利益相較於當事人之利益較為重要。

（2）於第 1 項所定情形，應採行適當及特定措施維護當事人之法益。考量技術之發展情形，採行之成本，處理之形式、範圍、狀態及目的，以及因處理而對當事人自由權利所招致風險之各種發生可能性與嚴重性，其特別可能包括：

1. 採行技術及組織上之措施，以確保依據 GDPR 而為之處理得以完成，
2. 確保事後審查及得以確認，個人資料是否以及由何人交付、變更或移除之措施，
3. 使處理過程中之參與者敏感化，
4. 任命個資保護長
5. 將近用個人資料之範圍限於資料控管者及受託處理者之所在範圍內，
6. 將個人資料假名化，
7. 將個人資料加密，
8. 確保與處理個人資料有關之系統及服務之能力、可信度、完整性、可用性與持久性，包括其在物理上或技術上突發狀況下迅速回復之能力、可用性及取得，
9. 為維護處理之安全性，就技術性及組織性措施之有效性，建立經常性之查核、評估及評等之程序，
10. 確保就目的外之處理或傳輸訂定之特殊程序規範，符合本法以及 GDPR 要求。

第 23 條 公務單位之目的外處理

（1） 透過公務單位，基於與蒐集目的不同之其他目的處理個人資料，應於其履行任務之範圍內，方得許之，且當其

1. 顯然係為維護當事人法益，且無理由認為當事人知悉該其他目的可能會拒絕同意，
2. 必須審核當事人之陳述，因事實上足認其正確性有疑慮，

3. 為防止對公共利益之重大損害或對公共安全、軍事防衛或國家安全之危害，或為維護公眾之重大利益或為確保稅務及海關收益所必要，
4. 為追訴犯罪或追究違反秩序之行為，為強制執行或執行刑法第 11 條第 1 項第 8 款所定刑罰或措施、少年法院法所定感化教育或教養方法或為強制執行罰金所必要，
5. 為防止對他人權利之嚴重損害所必要，
6. 為履行監督及管理之職權，審計查核或執行對控管者之組織調查；此亦適用於基於教育及考試之目的透過控管者而為處理之情形，且與當事人值得保護之法益未有牴觸。

（2）就 GDPR 第 9 條第 1 項所稱特種個人資料，採行與蒐集目的不同之其他目的之處理，應具備第 1 項所定要件以及 GDPR 第 9 條第 2 項或第 22 條所定例外要件，方得許之。

第 24 條 非公務單位之目的外處理

（1）透過非公務單位，基於與蒐集目的不同之其他目的處理個人資料，得允許之，當其
1. 係為防止對國家或公共安全之危害或為追訴犯罪所必要或
2. 係屬為適用、主張民法上請求權或為對抗民法上請求權所必要，

且於此範圍內當事人就排除處理未有更值得保護之利益。

（2）就 GDPR 第 9 條第 1 項所稱特種個人資料，採行與蒐集目的不同之其他目的之處理，應具備第 1 項所定要件以及 GDPR 第 9 條第 2 項或第 22 條所定例外要件，方得許之。

第 26 條 基於就業關係目的之資料處理

（1）基於就業關係目的得處理勞動者之個人資料，當其對於決定成立

就業關係，或於成立就業關係後之契約履行或終止，或勞動者之利益代表為主張或履行依據本法或集體契約或企業或職務約定（團體協約）所享有之權利及義務所必要者。為舉發犯罪得處理勞動者之個人資料，當經記錄之事實上證據顯示當事人於就業關係中有犯罪之嫌疑，而該處理係屬舉發犯罪所必要且勞動者於排除個人資料處理並未享有更值得保護之利益，特別是其方式及範圍與其動機間並未不合比例。

（2）依據當事人之同意處理勞動者之個人資料，於判斷是否為自願同意時，應特別關注就業關係中勞動者之從屬性以及給予同意之環境。當勞動者因而取得法律上或經濟上優勢或雇主與勞動者追求之法益相同時，特別得認定屬自願。除非因特殊情況而以採用其他形式為當，同意應以書面或電子之形式為之。雇主應向勞動者以文字形式說明關於資料處理之目的以及其依據GDPR第7條第3項得主張之撤回權。

（3）排除GDPR第9條第1項之適用，基於就業關係之目的處理GDPR第9條第1項所稱特種個人資料，於其係為行使權利或履行勞動法上之法定義務、社會安全及社會保護所必要，且未有理由支持，存在當事人因排除該處理所得獲致之法益較值得保護之例外情況時，方得為之。對於特種個人資料處理之同意，第2項亦有其適用；該同意必須清楚地指明所欲處理之資料。第22條第2項準用之。

（4）個人資料之處理，包括基於就業關係之目的處理勞動者之特種個人資料，得依據團體協約為之。於此談判代表應留意GDPR第88條第2項之規定。

（5）控管者應採行適當措施，以特別確保GDPR第5條所定基本原則於個人資料之處理中被遵守。

（6）勞動者權益代表之參與權不受影響。

（7）當勞動者之個人資料之處理，包括特種個人資料，並未儲存或未

應被儲存於於資料系統中時，第 1 項至第 6 項亦有其適用。

（8）本法所稱勞動者係指：

1. 勞工，包括與雇主簽約之臨時工作者；
2. 為了職業教育而工作；
3. 為了參與勞動生活、參加職業傾向之確認或參與試作而提供勞務之參與者（重返就業者）；
4. 於經認可之機構為身心障礙者工作；
5. 依據青少年自願服務法（Jugendfreiwilligendienstgesetz）或聯邦自願服務法（Bundesfreiwilligendienstgesetz）提供自願服務者；
6. 因經濟上獨立性而被視為具有類似雇主地位者包括在家工作和與其相當者；
7. 聯邦公務員、聯邦法官、軍人及服替代役者。

應徵前述就業關係之人，以及就業關係已終結之人，均屬本法所稱勞動者。

第 27 條 基於科學或歷史研究目的以及統計目的之資料處理

（1）排除 GDPR 第 9 條第 1 項之適用，即使未經同意，亦得基於科學或歷史研究目的以及統計目的，處理 GDPR 第 9 條第 1 項所稱特種個人資料，當該處理係達成目的所必要，且控管者因處理所獲致利益顯然高於當事人因不處理所得獲致利益。管理者應依據第 22 條第 2 項第 2 句採行適當且特定之措施，維護當事人之權益。

（2）當事人依據 GDPR 第 15 條、第 16 條第 18 條及第 21 條所享有之權利受有一定程度之限制，當其可能導致研究或統計之目的無法實現或造成嚴重的妨礙，且此一限制乃係為達成研究或統計目的所必要。當事人於其資料係屬科學研究目的所必須且答覆查詢將導致不合比例之費用時，不得依據 GDPR 第 15 條主張近用權。

（3）補充第 22 條第 2 項所稱措施，基於科學或歷史研究目的或統計

目的處理 GDPR 第 9 條第 1 項所稱特種個人資料，在對於研究或統計目的屬可能之範圍內，應將其匿名化（anonymisieren），除非其有違當事人之正當利益。於此之前，應就關於特定或可得特定當事人之屬人或屬事事項之個別資料，分開儲存。其僅得於研究或統計目的所必要之範圍內，將該個別資料予以彙整。

（4）僅於當事人同意或其對於呈現關於時代歷史事件之研究成果屬絕對必要時，控管者方得公開個人資料。

第 28 條 基於公共利益之檔案儲存目的之資料處理

（1）排除 GDPR 第 9 條第 1 項之適用，基於公共利益之檔案儲存目的處理 GDPR 第 9 條第 1 項所稱特種個人資料，於其屬達成公共利益之檔案儲存目的所必要時，方得為之。控管者應依據第 22 條第 2 項第 2 句採行適當且特定之措施，維護當事人之權益。

（2）若檔案並非透過當事人之姓名作成或並未提供得以合理之行政費用查找相關檔案之說明時，當事人不得依據 GDPR 第 15 條主張近用權。

（3）當該個人資料係基於公共利益之檔案儲存目的而處理時，當事人不得依據 GDPR 第 16 條主張更正權。若當事人對於個人資料之正確性有所爭執，應許其有為不同表述之機會。該檔案負有將此不同表述附加至檔卷之義務。

（4）依據 GDPR 第 18 條第 1 項第 a 款、第 b 款及第 d 款，第 20 條及第 21 條所享有之權利不得主張，當其可能導致基於公共利益之檔案儲存目的無法實現或造成嚴重的妨礙，且此一例外乃係為達成此目的所必要者。

第 30 條 消費借貸

（1）單位之業務上個人資料，係得利用於對消費者進行信用評等，並基於傳遞之目的而為蒐集、儲存或變更者，其對於來自歐盟其他

會員國之貸與人所提出查詢請求，應給予與本國之貸與人相同之待遇。

（2）若欲與消費者簽訂消費借貸契約或關於財務紓困契約，卻因第 1 項所稱單位所提供之查詢結果而予以拒絕時，應立刻通知消費者以及其所收到之查詢結果。若通知可能造成公共安全或秩序之危害時，則無須通知。第 37 條不受影響。

第 31 條 於計分及償付能力查詢之經濟交易保護

（1） 基於與特定人簽訂、執行或終止契約之目的，使用對其未來特定行為發生概然率之數值（計分），僅得於以下所列要件均符合時，方得為之：

1. 遵守個人資料保護法制之規定，
2. 計算概然率數值所利用之個人資料係依據科學認可之數學－統計方法可證明就該特定行為所計算之概然率數值屬顯著，
3. 概然率數值之計算並未僅利用地址資料，以及
4. 於利用當事人地址資料之情形，已於計算概然率數值之前即已通知其預計利用該等資料之情形；該通知應紀錄之。

（2）使用查詢機構所提供關於自然人償付能力及意願之概然率數值（償付能力查詢），於取得有關債權資訊之情況中，得允許之，若其具備第 1 項所定要件，且該債權限於債務屆期未履行，並

1. 由確定判決或目前宣告執行之判決所確認或依據民事訴訟法第 794 條具有債務名義，
2. 符合破產法第 178 條且於審查期日未為債務人所爭執，
3. 經債務人明確承認，
4. 就此債權
   a) 對債務人於屆期後就債權至少為二次書面警告，
   b) 第一次警告至少於四週前作成，
   c) 債務人先前，但最早於第一次警告時，已由詢問機構告知可

能之注意事項，

d) 債務人對此債權並不爭執，或

5. 其所依據之契約關係由於延遲繳納得不受期限拘束解除且債務人先前就可能應注意之事項已經詢問機構通知。

允許處理之範圍，包括傳遞概然率數值，其他依據一般個人資料保護規定所為與償付能力查詢相關之個人資料的處理則不受影響。

第 32 條 直接向當事人蒐集個人資料之告知義務

（1）GDPR 第 13 條第 3 項所定向當事人為告知之義務，除 GDPR 第 13 條第 4 項所稱例外以外，關於預計再處理時之告知義務，亦不適用於

1. 對於類似已儲存個人資料之再處理，若控管者係透過再處理直接將該資料用於當事人，且該再處理之目的與原始蒐集目的具有一致性，且其與當事人之溝通並非運用數位形式，而當事人於受告知所得獲致之法益，以資料蒐集之整體關聯性觀察，於各別情況中屬較為輕微，
2. 對於公務單位依法履行依據 GDPR 第 23 條第 1 項第 a 款至第 e 款對於控管者因其職權所生任務可能造成危害，且控管者不告知所得維護之法益，較當事人之法益值得保護，
3. 妨害公共安全或秩序或對於聯邦或邦之福祉可能導致不利益，且控管者因不告知所得維護之法益，較當事人之法益更值得保護，
4. 對於法律上請求權之適用、行使或防衛可能造成妨害，且控管者因不告知所得維護之法益，較當事人之法益值得保護，或
5. 可能造成向公務單位秘密傳輸資料之妨害。

（2）依據第 1 項免除告知義務之情況，控管者應相應採行適當措施維護當事人之正當利益，包括以更明確、更透明、更易於理解且更

易於取得之形式，以清楚並簡易之文辭，對外公開 GDPR 第 13 條第 1 項及第 2 項之告知事項。控管者對於其得以免除告知義務之原因，應以書面記錄之。第 1 句及第 2 句於第 1 項第 4 款及第 5 款不適用之。

（3）若第 1 項免除告知義務之情況，係因暫時性之障礙所導致，控管者應考量該特殊處理情形，於該暫時無法為告知之原因消失後，於適當期間補行告知，最長不得逾二星期。

第 33 條 間接向當事人蒐集個人資料之告知義務

（1）GDPR 第 14 條第 1 項、第 2 項及第 4 項所定向當事人為告知之義務，除 GDPR 第 14 條第 5 項及本法第 29 條第 1 項第 1 句所定例外之外，亦不適用，當該告知

1. 於公務單位之情形

a) 對其依法履行依據 GDPR 第 23 條第 1 項第 a 款至第 e 款因控管者職權所生任務可能造成危害，或

b) 妨害公共安全或秩序或對於聯邦或邦之福祉可能導致不利益

以及當事人因告知所生利益於此應退讓。

2. 於非公務單位之情形

a) 可能妨害民事上請求權之適用、行使或防衛，或處理之資料係來自於民事契約中且係為預防因刑事犯罪所生損害，而當事人於受告知所得獲致之正當利益，並未具有優勢，或

b) 經專責公務單位認定，控管者公布資料可能危害公共安全或秩序或可能對於聯邦或邦之福祉招致不利益時；但基於刑事追訴目的所為資料處理，則無須經前述確認。

（2）依據第 1 項免除告知義務之情況，控管者應相應採行適當措施維護當事人之正當利益，包括以更明確、更透明、更易於理解且更易於取得之形式，以清楚並簡易之文辭，對外公開 GDPR 第 14

條第 1 項及第 2 項之告知事項。控管者對於其得以免除告知義務之原因，應以書面記錄之。

（3）針對公務單位基於國家安全目的傳遞資料予特定機關，如憲法保護機關、聯邦情報機關、軍事防護勤務單位以及涉及聯邦安全之其他聯邦國防部所屬機關，則關於該傳遞之告知，僅得於獲得該等機關之同意下，方得為之。

第 34 條 當事人之近用權

（1）GDPR 第 15 條所定近用權，除第 27 條第 2 項、第 28 條第 2 項及第 29 條第 1 項第 2 句所定例外情形外，亦不適用，當

1. 依據德國個資法第 33 條第 1 項第 1 款、第 2 款第 b 目或第 3 項之規定，無須告知當事人，或
2. 該資料

a)係僅係因依據法律或命令所定儲存規定無法刪除，而因此儲存者，或

b)專為達成資料安全或資料保護控管之目的

且該查詢將可能須花費不合比例之費用並採行適當之技術及組織上措施排除目的外處理之可能。

（2）拒絕提供查詢之理由應紀錄之。關於作成拒絕查詢決定之事實上或法律上理由，若不會對拒絕查詢所欲達成之目的造成妨礙時，應即告知當事人。為了達成提供當事人查詢之目的以及為此準備而儲存之資料，僅得於此目的內以及為資料控管之目的為處理；出於其他目的所為處理，受 GDPR 第 18 條關於限制處理權之限制。

（3）若當事人於聯邦之公務單位未獲查詢，且其非屬經聯邦最高專責機關確認，可能妨害聯邦或邦之安全的各別情形時，則其應依請求告知聯邦監察官。由聯邦監察官告知當事人關於個人資料保護

法上審查之結果中，若其並非屬廣泛之查詢，不應包含控管者判別之推論。

（4）當事人對於其受公務單位既非以自動化方式處理，亦非屬以非自動化方式處理並儲存於資料系統中之個人資料時，僅得於當事人足以釋明該資料產生之可能以及提供查詢所生必要費用未與當事人因公開所得獲致之資訊利益不符比例情況下，方得主張個人資料之近用權。

第 35 條 刪除權

（1）針對以非自動方式處理個人資料之刪除，若因其特殊之儲存形式無法刪除或須花費不成比例之高額費用方屬可能，且當事人因刪除所得受保護之法益屬較輕微者，則補充 GDPR 第 17 條第 3 項所定例外情形，不適用 GDPR 第 17 條第 1 項所定當事人之刪除權與控管者之刪除義務。於此情形對於刪除之單位適用有關 GDPR 第 18 條所定限制處理之規定。第 1 句及第 2 句於個人資料非法處理之情況下不適用之。

（2）補充 GDPR 第 18 條第 1 項第 b 款及第 c 款，於 GDPR 第 17 條第 1 項第 a 款及第 d 款之情況，若控管者有理由認為，刪除將可能導致當事人應受保障之法益受到影響，則準用第 1 項第 1 句及第 2 句之規定。就處理之限制，若該通知並非不可能或未顯示可能須耗費不成比例之費用，控管者應通知當事人。

（3）補充 GDPR 第 17 條第 3 項第 b 款之規定，於 GDPR 第 17 條第 1 項第 a 款所定情形下，當刪除與法令或契約所定保留期限相互牴觸時，準用第 1 項之規定。

第 36 條 拒絕權

GDPR 第 21 條第 1 項之拒絕權，當該個人資料之處理具有急迫公共利益，且其較當事人之法益更值得保護，或該處理係法規明

定之義務時，不得向公務單位主張之。

第 37 條 個案中之自動化決策，包括剖析

（1） GDPR 第 22 條第 1 項所定任何人有權不接受僅基於自動化處理而作成之決定，其於 GDPR 第 22 條第 2 項第 a 款及第 c 款中所定之例外情況不適用，當該決定涉及依據保險契約所提供之給付範圍且

1. 已經當事人同意或
2. 該決定與實施對治療行為具拘束力收費規定相關且控管者對於該申請並未獲得充分同意之情形，採取適當之措施以維護當事人之正當利益，於此至少包括獲知代表控管者之人的權利、陳述自身觀點之權利以及撤銷該決定之權利；控管者至遲於獲知該申請未獲當事人充分同意之時，通知當事人關於該等權利

（2） 依據第 1 項作成之決定得處理 GDPR 第 4 條第 15 款所稱健康資料。管理者應採行第 22 條第 2 項第 2 句所定適當且特定措施以維護當事人之利益。

第 38 條 非公務單位之個資保護長

（1）補充歐盟第 2016/679 號規則第 37 條第 1 項第 b 款及第 c 款之規定，控管者及受託處理者若通常設置至少有 20 人以上專責自動化處理個人資料者，應任命一名個資保護長。若控管者及受託處理者預計採行之資料處理，依據歐盟第 2016/679 號規則第 35 條應採行資料保護影響評估，或是其業務上基於傳送、匿名傳送(anonymisierte Übermitteilung)之目的或進行市場或意見調查之目的而處理個人資料時，則不受資料受託處理者數量之限制，均應任命個資保護長。

（2）第 6 條第 4 項、第 5 項第 2 句以及第 6 項之規定準用之，第 6 條

第 4 項僅於負有任命個資保護長之義務時，方準用之。

第 40 條 邦之監督機關

（1） 依據邦法所設立之專責機關，主責監督於GDPR適用之範圍內，非公務單位就個人資料保護規定之適用。

（2） ……

附錄二 英國 2018 年資料保護法部分條文翻譯

第 10 條 個人資料和刑事定罪等資料的特殊類別

（1）於（2）和（3）項規定之 GDPR 第 9 條第 1 項（禁止處理特殊類別的個人資料）中所述的個人資料的處理，以下列條款之一為第 9 條第 2 項之例外情況—

(a)（GDPR 第 9 條第 2 項）第 b 款（就業、社會保障和社會保護）；

(b)（GDPR 第 9 條第 2 項）第 g 款（重大公共利益）；

(c)（GDPR 第 9 條第 2 項）第 h 款（衛生和社會保健）；

(d)（GDPR 第 9 條第 2 項）第 i 款（公共衛生）；

(e)（GDPR 第 9 條第 2 項）第 j 款（存檔、研究和統計）

（2）只有在基於滿足符合附件 1 第 1 部分的要件或因此得到英國部分法律的授權，（個資）處理才得符合 GDPR 第 9 條 2 項第 b、h、i 或 j 款的要求。

（3）…

第 11 條 個人資料等特殊類別：補充

（1） 為達成 GDPR 第 9 條第 2 項第 h 款（出於健康或社會護理目的而進行的處理等）之目的，進行個人資料處理之情狀應符合 GDPR 第 9 條第 3 款（保密義務）之構成要件和保護措施，包括：

(a) 由衛生專業人員或社會工作專業人員承擔或由其負責，或

(b) 其他在該情況下根據成文法或法律規定負有保密義務之人。

（2）在 GDPR 第 10 條和（本法）第 10 條中，提及與前科及犯罪有關的個人資料或相關的安全措施包括與以下有關的個人資料：

(a) 當事人所指控的犯罪行為，或

(b) 針對當事人所犯或據稱已犯的罪行的訴訟，或處置此類訴訟程序，包括量刑。

第 14 條 法律授權的自動化決策：安全維護措施

（1）本條係基於 GDPR 第 22 條第 2 項第 b 款之目的而為規範（即 GDPR 第 22 條第 1 項的例外情況，係依據法律授權所為，僅基於自動化處理所成的重大決策，並對當事人的權利、自由和正當利益有安全維護措施）。

（2）就本條言，一項決策對當事人而言，符合下列要件，則是「重大決策」 —

(a) 對當事人產生法律效果，或

(b) 對當事人產生類似重大影響。

（3）就本條言，一項決策對當事人而言，符合下列要件，則是「準重大決策」 —

(a) 是關於當事人的一項重大決策，

(b) 係法律要求或授權，並且

(c) 不屬於 GDPR 第 22 第 2 項第 a 款或第 c 款之規定（為契約或在當事人的同意下必要達成之決定）

（4）當控管者僅基於自動化處理就當事人而為準重大決策，則—

(a) 控管者必須在合理可行的範圍內盡快以書面通知當事人關該決策係僅基於自動化處理所做成，並且

(b) 當事人得於收到通知起 1 個月期間內，要求控管者-

i. 重新考慮該決策，或

ii. 做出不完全基於自動化處理的新決策。

（5）...

第 19 條 用於檔案儲存、研究和統計目的之處理：保障措施

（1）本節規定-

(a) 處理出於公共利益而存檔所需的個人資料

(b) 處理出於科學研究或歷史研究目的所必需的個人資料，以及

(c) 處理出於統計目的所需的個人資料。

（2）如果該處理很可能對當事人造成重大損害或嚴重困擾，則這樣的處理不符合 GDPR 第 89 條第 1 項必須對當事人的權利和自由採取適當的保障措施的要求。

（3）除非必要的處理目的包括批准的醫學研究的目的，否則如果出於針對特定當事人的措施或決策目的執行處理，則此類處理不滿足該要求。...

第 45 條 當事人之近用權

（1）當事人有權從資料控管者獲取以下資訊：

(a) 關於是否正在處理有關他或她的個人資料的確認，並且

(b) 在這種情況下，近用第（2）項中列出的個人資料和資訊。

（2）該資訊是-

(a) 處理的目的和法律依據；

(b) 有關個人資料的類別；

(c) 被揭露個人資料所針對的接收者或接收者類別（包括第三國或國際組織的接收者或接收者類別）；

(d) 預計將儲存個人資料的期限，或者在不可能的情況下，用於確定該期限的標準；

(e) 是否存在當事人有權要求資料控管者提出的權利-

i. 更正個人資料（請參閱第 46 條），以及

ii. 刪除個人資料或限制其處理（請參閱第 47 條）；

(f) 是否存在當事人向資訊委員提出投訴的權利以及資訊委員的聯繫方式；

(g) 溝通正在處理的個人資料以及有關其來源的任何可用資訊。

（3）凡當事人根據第（1）項提出要求，該當事人有權獲得的資料必須以書面提供-

(a) 不得無故延遲，並且

(b) 在任何情況下，均應在適用期限結束之前（參見第 54 條）。

（4）在考慮到當事人的基本權利和正當利益的前提下，資料控管者可以全部或部分限制第（1）項授予的權利，只要該限制是必要的和相稱的措施即可-

(a) 避免妨礙官方或法律的詢問、調查或程序；

(b) 避免損害對刑事犯罪的預防、偵查、調查、起訴或執行刑事處罰；

(c) 保護公共安全；

(d) 保護國家安全；

(e) 保護他人的權利和自由。

（5）凡第（1）項所指當事人的權利受到全部或部分限制，則資料控管者必須以書面通知當事人，不得無故拖延-

(a) 當事人的權利受到限制，

(b) 限制的原因，

(c) 當事人根據第 51 條向資訊委員提出請求的權利，

(d) 當事人有權向資訊委員提出投訴，以及

(e) 當事人根據第 167 條向法院申請的權利。

（6）第（5）（a）和（b）項不適用於提供資訊會破壞限制目的之程度。

（7）資料控管者必須-

(a) 記錄根據第（1）項限制（全部或部分）當事人權利的決定的理由，以及

(b) 如資訊委員要求，則將該紀錄提供予該資訊委員。

第 46 條 當事人之更正權

（1）如果當事人有此要求，則資料控管者必須立即更正與該當事人有關的不正確的個人資料。

（2）如果由於個人資料不完整而導致個人資料不正確，則如果當事人要求，資料控管者必須完成個人資料。

（3）在適當情況下，第（2）項所指的職責可通過提供補充說明加以履行。

（4）出於證據目的留存個人資料，如果根據本條要求資料控管者更正個人資料，則資料控管者必須（而不是更正個人資料）限制其處理。

第 47 條 當事人之刪除權與限制處理權

（1）若有以下情況，資料控管者必須立即刪除個人資料：

(a) 處理個人資料將違反第 35、36（1）至（3）條、37、38（1）、39（1）、40、41 或 42 條，或

(b) 資料控管者有刪除資料的法律義務。

（2）如果根據第（1）項要求資料控管者刪除個人資料，但必須出於證據目的保留個人資料，則資料控管者必須（而不是刪除個人資料）限制其處理。

（3）如果當事人對個人資料的準確性提出質疑（無論是根據本節或第 46 條提出請求，還是以任何其他方式提出），但無法確定其準確性與否，則資料控管者必須限制其處理。

（4）當事人可能會要求資料控管者刪除個人資料或限制其處理（但

無論是否提出這種要求，資料控管者在本條中的職責均適用）。

第 49 條 拒絕受自動化作成決策權

（1）除非法律要求或授權，否則資料控管者不得僅基於自動化處理做出重大決策。

（2）就本條而言，以下決策是一項「重大決策」：

(a) 對當事人產生不利的法律效果，或

(b) 對當事人有重大影響。

第 50 條 法律授權得為自動化作成決策權

（1） 就本條而言，一項決定是「準重大決策」之定義如下 —

(a) 這是與當事人有關的重大決策，並且

(b) 法律要求或授權。

（2） 如果資料控管者僅基於自動化處理就當事人做出準重大決策，則

(a) 資料控管者必須在合理可行的範圍內盡快以書面通知當事人已完全基於自動化處理做出的決策，並且

(b) 當事人得於收到通知起 1 個月期間內，要求資料控管者-

i. 重新考慮該決策，或

ii. 做出不完全基於自動化個資處理的新決策。...

第 69 條 指定（一名）個資保護長

（1） 除非資料控管者是以法院身分行事的法院或其他司法機構，否則資料控管者必須指定一名個資保護長。

（2） 在指定個資保護長時，資料控管者必須考慮個資保護長的專業素質，尤其是：

(a) 個資保護長對資料保護法律和實踐的專業知識，以及

(b) 個資保護長執行第 71 條所述任務的能力。

（3） 考慮其組織結構和規模，同一個人可能被多個資料控管者指定為個資保護長。

（4） 資料控管者必須發布個資保護長的聯繫方式，並將其告知資訊委員。

第 70 條 個資保護長之職位

（1） 資料控管者必須確保個資保護長正確，及時地介入與個人資料保護有關的所有問題。

（2） 資料控管者必須向個資保護長提供必要的資源，並可以近用個人資料和處理操作，以使個資保護長能夠-

(a) 執行第 71 條所述的任務，以及

(b) 保持他或她對資料保護法的專業知識以及實踐。

（3） 資料控管者-

(a) 必須確保個資保護長不會收到任何有關第 71 條執行任務的指示；

(b) 當個資保護長執行任務或履行本部分以外職務導致利益衝突時，必須確保個資保護長不執行該任務或該職務；

(c) 不得解僱或懲罰個資保護長執行第 71 條所述的任務。

（4） 當事人可以就以下所有問題與個資保護長聯繫：

(a) 處理該當事人的個人資料，或

(b) 該當事人在本部分中的權利的行使。

（5） 個資保護長在擔任此職務時必須向資料控管者的最高管理層級報告。

第 71 條 個資保護長之任務

（1） 資料控管者必須至少委託個資保護長執行以下任務：

(a) 告知資料控管者、資料控管者聘用的任何受託處理者以及進行個人資料處理的資料控管者的任何員工有關該人在本部分中的義務，

(b) 就根據第 64 條進行的個資保護影響評估提供諮詢意見，並監督其遵守情況，

(c) 與資訊委員合作，

(d) 擔任資訊委員關於個資處理的聯絡窗口，包括與第 65 條所述的諮詢有關，並在適當情況下與資訊委員就任何其他事項進行諮詢，

(e) 監控與資料控管者有關個人資料保護政策的合規性，以及

(f) 監控資料控管者對本部分的遵守情況。

（2） 關於第（1）(e）款中提到的政策，個資保護長的任務包括：

(a) 根據這些政策分配職責，

(b) 提高對這些政策的認識，

(c) 訓練從事個資處理業務的人員，以及

(d) 進行這些政策要求的審核。

（3） 在執行第（1）和（2）款中規定的任務時，個資保護長必須考慮到與處理操作相關的風險,同時要考慮到處理的性質、範圍、背景和目的。

第 114 條 資訊委員

（1） （承繼 DPA 1997）仍有一個資訊委員。

（2） 附件 12 就資訊委員作出規定。

第 116 條 （資訊委員之）其他職權

（1） 資訊委員—

(a) 就「(歐盟) 執法指令(Law Enforcement Directive)」第 41 條而言，是英國的監管機構，並且

(b) 就「(歐洲理事會) 個資保護公約」第 13 條而言，仍將繼續是英國的指定機關。

(2) 附件 13 賦予資訊委員不適用 GDPR 而與個資處理相關的一般職權（另請參見資訊委員根據第 2 條的職責）。

(3) 本條和附件 13 不損害資訊委員根據本法或其他方式賦予的其他職權。

第 123 條 適合年齡的設計規範

(1) 資訊委員必須準備一份行為守則，其中載有資訊委員認為適當的指導，以指導可能適合兒童使用的相關資訊社會服務的年齡設計標準。

(2) 當本條所指的守則已生效，資訊委員可準備該守則之修訂或替代守則。

(3) 在根據本條準備守則或修正案之前，資訊委員必須諮詢國務卿和資訊委員認為適當的其他人員，包括-

(a) 兒童，

(b) 父母，

(c) 資訊委員所認定代表兒童利益的人，

(d) 兒童發展專家，以及

(e) 商業團體。

(4) 資訊委員在根據本條擬具守則或修訂時，必須考量—

(a) 兒童在不同的年齡有不同的需求，並且

(b) 履行英國在「聯合國兒童權利公約」下的義務。

(5) 本條所指的守則可包括過渡性條文或保留條文。

(6) 根據本條第一項守則所包含的任何過渡性規定，必須在守則生

效後的 12 個月期限內停止生效。

（7） …

第 171 條 對去識別化個資進行再識別

（1） 個人因故意或過失對於已去識別化之個資，在未經資料控管者就該等去識別化個資負有法律責任範圍內同意之情況下，將之再識別而得出資訊則係為刑事之犯罪。

（2） 為本條與第 172 條之目的：

(a) 去識別化指無法將該等資料歸屬於特定之當事人；

(b) 再識別定義為個人以方法造成該等資訊無法再處於前述去識別化之定義狀態下。

（3） 如能證明以下事由，則阻卻第(1)項之違法：

(a) 防止或偵查犯罪之目的所需而具有必要性；

(b) 授權機關為執行法律、依法或是依據法院令狀之所需；

(c) 為特定情況下為公共利益而為之。

（4） 如能證明以下事由，則亦能阻卻第(1)項之違法：

(a) 為再識別之人之行為係合理信賴其

i. 本身即是該等個資之當事人；

ii. 經當事人同意；[314]

iii. 如果當事人知道在該等情狀下會被再識別時，一定會予以同意。

(b) 為再識別之人之行為係合理信賴其

i. 係為需負擔法律責任之資料控管者；

ii. 經資料控管者同意；

iii. 如果資料控管者知道在該等情狀下會被再識別時，一定會

[314] 須注意者，DPA 2018 第 171 條(8)特別說明，在 171 條各款的同意中，不包含 GDPR 第 28 條(10)，以及 DPA 2018 第 59(8)、105(3)條之同意。

予以同意。

(c) 為再識別之人之行為

i. 係為特殊目的；

ii. 為新聞、學術、藝術或文學作品之出版；

iii. 合理信賴其再識別係在特定情狀下為了公共利益，且可被正當化。

(d) 符合第 172 條之有效性測試構成要件(effectiveness testing conditions)

（5） 任何人意圖或魯莽地(未必故意或有認識過失)處理個人資料，即在再識別該等資訊，即屬犯罪：

(a) 未經負責去識別個人資料的資料控管者同意，

(b) 並且在根據第（1）項重新識別為犯罪的情況下為之。

（6） 第（5）項犯罪之阻卻事由為：

(a) 為預防或偵查罪行所必需，

(b) 並且在根據第（1）項重新識別為犯罪的情況下為之。

(c) 在特定情況下，被認為符合公共利益。

（7） 如能證明以下事由，則亦能阻卻第(5)項之違法：

(a) 該行為人有合理理由相信該處理是合法的，

(b) 該行為人有合理理由相信其—

i. 得到負責取消識別個人資料的控管者的同意，或

ii. 如果該控管者知道其處理過程和情況,則本應獲得該同意，或

(c) 該行為人之行為—

i. 出於特殊目的，

ii. 為使某人發表任何新聞、學術、藝術或文學材料，以及

iii. 合理認為，在特定情況下，該處理被認為符合公共利益。

（8） 在本條中：

(a) 關於資料控管者之同意不包括依 GDPR 第 28 條第 10 項或本法第 59 條第 8 項或第 105 條第 3 項成為控管者的人（在某些情況下被視為資料控管者）

(b) 如資料控管者不止一個，則該同意是對其中一個或多個同意的同意。

第 172 條 有效性測試構成要件(effectiveness testing conditions)

（1） 就第 171 條而言，對於再識別被去識別化的個人資料的資訊之人而言，「有效性測試構成要件」是指第（2）和（3）項中的條件。

（2） 該為再識別之人之行為同時符合下列三者：

(a) 係在測試該等去識別化個資之效果（例如侵入者亂度測試等）；

(b) 並非為了意圖造成威脅傷害或侵擾其他個人；

(c) 具合理信賴其再識別係在特定情狀下為了公共利益，且可被正當化。

（3） 該行為人通知資訊委員或是需負擔法律責任之資料控管者，並符合

(a) 未有遲延，且

(b) 於可預見情狀下，不晚於 72 小時。

（4） 如果有一個以上之資料控管者，僅需其中一人或以上被通知即可。

第 174 條 特殊目的

（1） 在本部分中，「特殊目的」是指以下一個或多個目的-

(a) 新聞目的；

(b) 學術目的；

(c) 藝術目的；

(d) 文學目的。

（2） 在本部分中，「特殊目的程序」是指針對控管者或受託處理者的法律程序，其全部或部分與為特殊目的而處理的個人資料有關，並且—

(a) 根據第 167 條提出的程序（包括根據 GDPR 第 79 條提出的申請程序），或

(b) 根據第 169 條或 GDPR 第 82 條進行的程序。

（3） 資訊委員得就以下處理個人資料作出書面決定—

(a) 並非僅出於特殊目的處理個人資料；

(b) 控管者未曾發表，且係個人基於發表新聞、學術、藝術或文學資料目的所為者，非屬個人資料之處理。

（4） 資訊委員必須將決定的書面通知控管者和受託處理者。

（5） 通知書必須提供有關根據第 162 條規定之上訴權的資訊。

（6） 該決定只有在滿足以下條件之一後才會生效—

(a) 在沒有提出上訴的情況下，控管者或受託處理者對該決定提出上訴的期限屆滿，或

(b) 已就該決定提出上訴，而—

i. 有關該決定的上訴和任何進一步的上訴已經確定或已經終止，並且

ii. 針對上訴結果或進一步上訴提出上訴的時間已經結束，而沒有再次提出上訴。

附錄三　　本報告所涉個人資料保護法制之比較

	我國	歐盟	德國	英國
監管機關之中央與地方權限	第 22 條 （無個資保護長之規範）	1. 監管機關之設立：第 51 條 2. 監管機關之獨立性：第 52 條 3. 監管機關之權限：第 56 條 4. 監管機關職務內容：第 57 條、第 58 條	1. 聯邦個人資料暨資訊自由監察官：第 4 章，第 8 條至第 16 條 2. 各邦之監督機關：第 40 條 3. 個資保護長 （1）公務單位：第 5 條至第 7 條 （2）非公務單位：第 38 條	1. 監管機關之設立：第 114 條、附件二 2. 監管機關之權限（與 GDPR 同）：第 115 條 3. 監管機關之權限（特有之一般性保障規範）：第 116 條、附件 13 4. 個資保護長：第 69、70、71 條
個資特定目的外利用之要件	1.公務機關:第 16 條 2.非公務機關:第 20 條	1. 特種個資：第 9 條第 2 項第 a 款至第 j 款，第 9 條第 4 項：允許	1. 特種個資 （1）公務單位：第 23 條第 2 項；	1. 特種個資：第 10、11 條，附件一 2. 一般個資:與 GDPR

		針對涉及基因、生物特徵或健康資料另作補充規範 2. 一般個資：第 6 條第 4 項	（2）非公務單位：第 24 條第 2 項 2. 一般個資： （1）公務單位：第 23 條第 1 項； （2）非公務單位：第 24 條第 1 項	同 *附件一第二部分明定公共利益類型與內涵
去識別化之要件、程序、認定方式等規定	1. 間接方式識別之定義：施行細則第 3 條 2. 無從識別之定義：施行細則第 17 條 3. 去連結：人體研究法第 4 條、人體生物資料庫管理條例第 3 條、第 18	假名化：第 4 條第 5 款	1. 特定適當措施 （1）特定適當措施之例示：第 22 條第 2 項 （2）特定適當措施之採行：第 23 條第 2 項、第 24 條第 2 項、第 26 條第 3 項、第 27 條第 1 項、第 28 條第 1 項、第 37 條第 2 項	1. 去識別化：第 171(2)(a)條 2. 再識別：第 171(2)(b)條、第 172 條

	條第 1 項 4. 加密：人體生物資料庫管理條例 第 3 條、第 18 條第 1 項 5. 編碼：人體生物資料庫管理條例 第 3 條、第 18 條第 1 項 6. 可逆之擬匿名化資料：法務部法律字第 10503505760 號函		2. 其他措施，如第 27 條第 3 項之「匿名化」及「分開儲存」 3. 監督機關共同訂定「個人資料保護模式之標準」供遵循	
特殊處理之情形	1. 公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計	1. 個人資料之處理與言論自由及資訊自由：第 85 條 2. 處理及公開官方檔	1. 基於就業關係目的之資料處理：第 26 條 2. 基於科學或歷史研究目的以及統計目的之	1. 個人資料之處理與言論自由及資訊自由：第 174 條 2. 處理及公開官方檔

	或學術研究(特種個資)：第 6 條第 1 項第 4 款 2. 公務機關或非公務機關基於公共利益為統計或學術研究之目的：第 9 條第 2 項第 4 款 3. 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：第 16 條第 5 款、第 20 條第 1 項第 5 款 4. （非公務機關的）學術研究機構基於公共利益為統	卷：第 86 條 3. 國家代碼之處理：第 87 條 4. 受雇者之資料處理：第 88 條 5. 保障基於公益之檔案儲存目的、基於學術或歷史研究目的以及統計目的之處理：第 89 條	資料處理：第 27 條 3. 基於公共利益之檔案儲存目的之資料處理：第 28 條 4. 消費借貸：第 30 條 5. 對於使用計分數值及支付能力查詢：第 31 條	卷：政府資訊公開法、環境資訊規則 3. 國家代碼之處理：英國無國家代碼（身分證）制度 4. 受雇者之資料處理：僱傭實務準則 5. 保障基於公益之檔案儲存目的、基於學術或歷史研究目的以及統計目的之處理：第 19 條

	計或學術研究：第19條第1項第4款 （無言論自由及資訊自由之調和規定、無與政資法之調和規定、無受雇者資料處理調和規定、無國家代碼處理調和規定）			
自動化機器作成之決定	無	第22條 自動化個人決策包含剖析	第37條 1. 限縮GDPR適用範圍 2. 允許使用健康資料	第14條，另有細部指引
當事人權利	1. 當事人權利：第3條 （1）查詢或請求閱覽 （2）請求製給複製	1. 當事人權利 （1）告知義務：第13、14條 （2）近用權：第15條 （3）更正權：第16條	1. 限縮GDPR當事人權利之適用： （1）告知義務：第32、33條 （2）近用權：第34條	1. 當事人權利 （1）近用權：第45條 （2）更正權：第46條 （3）刪除權、限制處理權：第47條

	本 （3）請求補充或更正 （4）請求停止蒐集、處理或利用 （5）請求刪除權 2. 未就兒童行使權利為特別規範	（4）刪除權：第 17 條 （5）限制處理權：第 18 條 （6）可攜權：第 20 條 （7）拒絕權：第 21 條 2. 涉及資訊社會服務時，兒童同意之要件：第 8 條	（3）刪除權：第 35 條 （4）拒絕權：第 36 條 2. 未規範關於兒童行使權利要件，直接適用 GDPR	（4）拒絕受自動化作成決策權：第 49、50 條 2. 關於兒童行使權利：第 123 條要求資訊委員做成「適合年齡設計準則」

附錄四 德國 2019 年 11 月 20 日因應 GDPR 第二次修法修正法規名稱

第一條：國籍法（Staatsangehörigkeitsgesetz, StAG）

第二條：規範因應兩德統一後加入聯邦社會保障體系地區所生財產問題保障法（Gesetz zur Regelung von Vermögensfragen der Sozialversicherung im Beitrittsgebiet, BGSVVermG）

第三條：聯邦安全檢核法（Sicherheitsüberprüfungsgesetz, SÜG）

第四條：反恐怖主義資料法（Antiterrordateigesetz, ATDG）

第五條：對抗法律極端主義資料法（Rechtsextremismus-Datei-Gesetz, RED-G）

第六條：歐盟簽證系統授權使用法（VIS-Zugangsgesetz , VISZG）

第七條：武器使用法（Waffengesetz, WaffG）

第八條：於數位傳播機關及組織就維安任務設置聯邦機構法（BDBOS-Gesetz, BDBOSG）

第九條：資訊公開法（Informationsfreiheitsgesetz, IFG）

第十條：公務員保障法（Beamtenstatusgesetz, BeamtStG）

第十一條：聯邦公務員法（Bundesbeamtengesetz, BBG）

第十二條：聯邦個人資料保護法（Bundesdatenschutzgesetz , BDSG）

第十三條：聯邦資訊安全維護局組織法（BSI-Gesetz, BSIG）

第十四條：電子郵件法（De-Mail-Gesetz, De-Mail-G）

第十五條：電子政府法（E-Government-Gesetz, EGovG）

第十六條：聯邦註冊登記法（Bundesmeldegesetz, BMG）

第十七條：身分登記法（Personenstandsgesetz, PStG）

第十八條：藥品法（Arzneimittelgesetz, AMG）

第十九條：藥品法及其相關規定第四次修正法（Vierten Gesetz zur Änderung arzneimittelrechtlicher und anderer Vorschriften, 4. AMGuaÄndG）

第二十條：輸血法（Transfusionsgesetz, TFG）

第二十一條：基因科技法（Gentechnikgesetz, GenTG）

第二十二條：麻醉製品基本原料管制條例（Grundstoffüberwachungsgesetz, GÜG）

第二十三條：基因測試法（Gendiagnostikgesetz, GenDG）

第二十四條：器官移植法（Transplantationsgesetz, TPG）

第二十五條：禁止運動賽事使用興奮劑法（Anti-Doping-Gesetz, AntiDopG）

第二十六條：酒品法（Weingesetz, WeinG）

第二十七條：煙草製品法（Tabakerzeugnisgesetz, TabakerzG）

第二十八條：食品、日用品及飼料管理法（Lebensmittel-und Futtermittel- gesetzbuch, LFGB）

第二十九條：醫院資金籌措法（Krankenhausfinanzierungsgesetz, KHG）

第三十條：傳染病保護法（Infektionsschutzgesetz, IfSG）

第三十一條：國際衛生法規執行法（IGV-Durchführungsgesetz, IGV-DG）

第三十二條：搜尋服務資料保護法（Suchdienstedatenschutzgesetz, SDDSG）

第三十三條：廢棄物運輸法（Abfallverbringungsgesetz, AbfVerbrG）

第三十四條：海事保險證據法(Seeversicherungsnachweisgesetz, SeeVersNachwG)

第三十五條：青少年志願服務法(Jugendfreiwilligendienstegesetz , JFDG)

第三十六條：防制婦女暴力救援專線法(Hilfetelefongesetz, HilftelefonG)

第三十七條：聯邦志願服務法(Bundesfreiwilligendienstgesetz , BFDG)

第三十八條：庇護者給付法(Asylbewerberleistungsgesetz, AsylbLG)

第三十九條：促進專業提升訓練法(Aufstiegsfortbildungsförderungsgesetz , AFBG)

第四十條：文化資產保護法(Kulturgutschutzgesetz , KGSG)

第四十一條：德國之聲法（Deutsche-Welle-Gesetz, DWG）

第四十二條：住宅促進法(Wohnraumförderungsgesetz, WoFG)

第四十三條：第二部興奮劑受害者協助法（Zweiten Dopingopfer-Hilfegesetz, DOHG2)

第四十四條：兩德統一前刑事受害者修復賠償法(Strafrechtlichen Rehabilitierungsgesetz, StrRehaG)

第四十五條：兩德統一前行政措施受害者修復賠償法(Verwaltungsrechtlichen Rehabilitierungsgesetz, VwRehaG)

第四十六條：兩德統一前職業受害者修復賠償法(Beruflichen Rehabilitierungsgesetz, BerRehaG)

第四十七條：外國人於中央機關辦理登記法(AZR-Gesetz, AZRG)

第四十八條：庇護法(Asylgesetz, AsylG)

第四十九條：居留法(Aufenthaltsgesetz, AufenthG)

第五十條：簽證警示資料法(Visa-Warndateigesetz, VWDG)

第五十一條：駐外人員法(Gesetze über den Auswärtigen Dienst, GAD)

第五十二條：聯邦中央登錄法(Bundeszentralregistergesetz, BZRG)

第五十三條：第七部聯邦中央登錄法（Siebten Gesetz zur Änderung des Bundeszentralregistergesetz, 7. BZRGÄndG）

第五十四條：歐洲司法合作機構組織法（Eurojust-Gesetz, EJG）

第五十五條：公海合作法（Hohe-See-Zusammenarbeitsgesetz, HSeeZG）

第五十六條：司法行政費用法（Justizverwaltungskostengesetz, JVKostG）

第五十七條：性工作者保護法（Prostituiertenschutzgesetz, ProstSchG）

第五十八條：證券交易法（Wertpapierhandelsgesetz, WpHG）

第五十九條：收購及發行有價證券法（Wertpapiererwerbs- und Übernahmegesetz, WpÜG）

第六十條：有價證券募集法（Wertpapierprospektgesetz, WpPG）

第六十一條：交易所法（Börsengesetz, BörsG）

第六十二條：刑法（Strafgesetzbuch, StGB）

第六十三條：打擊非法就業法（Schwarzarbeitsbekämpfungsgesetz, SchwarzArbG）

第六十四條：士兵法律地位法（Soldatengesetz, SG）

第六十五條：士兵平等待遇法（Soldatinnen- und Soldatengleichstellungsgesetz, SGleiG）

第六十六條：替代役法（Zivildienstgesetz, ZDG）

第六十七條：財政機關組織法（Finanzverwaltungsgesetz, FVG）

第六十八條：稅捐統計法（Gesetz über Steuerstatistiken, StStatG）

第六十九條：海關資料系統施行法（ZIS-Ausführungsgesetz, ZISAG）

第七十條：稅捐通則（Abgabenordnung, AO）

第七十一條：租捐通則施行法（Einführungsgesetz zur Abgabenordnung, EGAO）

第七十二條：1995 年連帶附加稅捐法（Solidaritätszuschlaggesetz 1995, SolzG 1995）

第七十三條：稅收諮詢法（Steuerberatungsgesetz, StBerG）

第七十四條：所得稅法（Einkommensteuergesetz, EStG）

第七十五條：營業稅法（Umsatzsteuergesetz, UStG）

第七十六條：賽馬博弈與彩券稅捐條例（Rennwett- und Lotteriegesetz, RennwLottG）

第七十七條：聯邦預算法（Bundeshaushaltsordnung, BHO）

第七十八條：金融集團重整與清算法（Sanierungs- und Abwicklungsgesetz, SAG）

第七十九條：會計師法（Wirtschaftsprüferordnung, WPO）

第八十條：能源統計法（Energiestatistikgesetz, EnStatG）

第八十一條：營利事業法（Gewerbeordnung, GewO）

第八十二條：產業及商業同業公會權益臨時法（Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern, IHKG）

第八十三條：醫療器材法（Medizinproduktegesetz, MPG）

第八十四條：手工業規範法（Handwerksordnung, HwO）

第八十五條：煙囪清掃從業人員執業及照護法（Schornsteinfeger-Handwerksgesetz, SchfHwG）

第八十六條：國家武器登記法（Nationales-Waffenregister-Gesetz, NWRG）

第八十七條：量測及計量法（Mess- und Eichgesetz, MessEG）

第八十八條：輻射保護法（Strahlenschutzgesetz, StrlSchG）

第八十九條：能源經濟法（Energiewirtschaftsgesetz, EnWG）

第九十條：測量操作法（Messstellenbetriebsgesetz, MsbG）

第九十一條：金融法（Kreditwesengesetz, KWG）

第九十二條：投資者賠償法（Anlegerentschädigungsgesetz, AnlEntG）

第九十三條：融資服務監理法（Finanzdienstleistungsaufsichtsgesetz, FinDAG）

第九十四條：支付服務監理法（Zahlungsdiensteaufsichtsgesetz, ZAG）

第九十五條：存款保險法（Einlagensicherungsgesetz, EinSiG）

第九十六條：投資法（Kapitalanlagegesetzbuch, KAGB）

第九十七條：無記名抵押債券法（Pfandbriefgesetz, PfandBG）

第九十八條：保險監理法（Versicherungsaufsichtsgesetz, VAG）

第九十九條：藥品折扣法（Gesetz über Rabatte für Arzneimittel, AMRabG）

第一百條：動物健康法（Tiergesundheitsgesetz, TierGesG）

第一百零一條：動物保護法（Tierschutzgesetz, TierSchG）

第一百零二條：肉品法（Fleischgesetz, FIG）

第一百零三條：市場組織法（Marktorganisationsgesetz, MOG）

第一百零四條：市場訂購商品通報法（Gesetz über Meldungen über Marktordnungswaren, MarktONOG）

第一百零五條：牛隻登記實施法（Rinderregistrierungsdurchführungsgesetz,RiRegDG）

第一百零六條：牛肉標示法（Rindfleischetikettierungsgesetz, RiFlEtikettG）

第一百零七條：農漁業基金資料法（Agrar- und Fischereifondsinformationen Gesetz, AFIG）

第一百零八條：於統一管理和控制系統中處理農業支付資料法（InVeKoS-Daten-Gesetz, InVeKoSDG）

第一百零九條：農業統計法（Agrarstatistikgesetz, AgrStatG）

第一百一十條：海洋漁業法（Seefischereigesetz, SeeFischG）

第一百一十一條：第五部置產法（Fünften Vermögensbildungsgesetz, 5. VermBG）

第一百一十二條：居家工作法（Heimarbeitsgesetz, HAG）

第一百一十三條：工作保護法（Arbeitsschutzgesetz, ArbSchG）

第一百一十四條：職業資格許可法（Berufsqualifikationsfeststellungsgesetz, BQFG）

第一百一十五條：跨境勞工法（Arbeitnehmer-Entsendegesetz, AEntG）

第一百一十六條：農民老年保險法（Gesetz über die Alterssicherung der Landwirte, ALG）

第一百一十七條：第二部農民健康保險法（Zweiten Gesetz über die Kranken- versicherung der Landwirte, KVLG 1989）

第一百一十八條：聯邦育兒津貼與育兒假法（Bundeselterngeld- und Elternzeitgesetz, BEEG）

第一百一十九條：社會法典第一部（Ersten Buch Sozialgesetzbuch, SGB I）

第一百二十條：社會法典第二部（Zweiten Buch Sozialgesetzbuch, SGB II）

第一百二十一條：社會法典第三部（Dritten Buch Sozialgesetzbuch, SGB III）

第一百二十二條：社會法典第四部（Vierten Buch Sozialgesetzbuch,

SGB IV）

第一百二十三條：社會法典第五部（Fünften Buch Sozialgesetzbuch, SGB V）

第一百二十四條：醫院收費法（Krankenhausentgeltgesetz, KHEntgG）

第一百二十五條：社會法典第六部（Sechsten Buch Sozialgesetzbuch, SGB VI）

第一百二十六條：老年照護契約認證法（Altersvorsorgeverträge-Zertifizierungsgesetz, AltZertG）

第一百二十七條：老年照護實施法（Altersvorsorge-Durchführungsverordnung, AltvDV）

第一百二十八條：社會法典第七部（Siebten Buch Sozialgesetzbuch, SGB VII）

第一百二十九條：社會法典第八部（Achten Buch Sozialgesetzbuch, SGB VIII）

第一百三十條：社會法典第九部（Neunten Buch Sozialgesetzbuch, SGB IX）

第一百三十一條：社會法典第十部（Zehnten Buch Sozialgesetzbuch, SGB X）

第一百三十二條：社會法典第十一部（Elften Buch Sozialgesetzbuch, SGB XI）

第一百三十三條：社會法典第十二部（Zwölften Buch Sozialgesetzbuch, SGB XII）

第一百三十四條：房租津貼法（Wohngeldgesetz, WoGG）

第一百三十五條：郵政法（Postgesetzes, PostG）

第一百三十六條：郵政服務之資料保護法（Postdienste-Datenschutzverordnung, PDSV）

第一百三十七條：道路交通法（Straßenverkehrsgesets, StVG）

第一百三十八條：駕駛員法（Fahrpersonalgesetz, FPersV）

第一百三十九條：汽車交通事故鑑定人法（Kraftfahrsachverständigengesetz, KfSachvG）

第一百四十條：危險貨品運輸法（Gefahrgutbeförderungsgesetz, GGBefG）

第一百四十一條：貨運運輸法（Güterkraftverkehrsgesetz, GüKG）

第一百四十二條：私人興建或捐助聯邦遠程交通道路法（Fernstraßenbauprivatfinanzierungsgesetz, FStrPrivFinG）

第一百四十三條：聯邦遠程交通道路收費法（Bundesfernstraßenmautgesetz, BFStrMG）

第一百四十四條:電子收費系統營運法(Mautsystemgesetz, MautSysG）

第一百四十五條：徵收使用基礎設施公課條例（Infrastrukturabgabengesetz, InfrAG）

第一百四十六條：內陸航行之聯邦任務法（Binnenschifffahrtsaufgabengesetz, BinSchAufgG）

第一百四十七條：海事任務法（Seeaufgabengesetz, SeeAufgG）

第一百四十八條：海上安全暨事故調查法（Seesicherheits-Untersuchungs- Gesetz, SUG）

第一百四十九條：歐盟船客權利法（EU-Fahrgastrechte-Schifffahrt-Gesetz, EU FahrgRSchG）

第一百五十條：船舶事故資料庫法（Schiffsunfalldatenbankgesetz, SchUnfDatG）

第一百五十一條：船員法（Seearbeitsgesetz, SeeArbG）

第一百五十二條：航空法（Luftverkehrsgesetz, LuftVG）

第一百五十三條：航空事故調查法（Flugunfall-Untersuchungs-Gesetz, FlUUG）

第一百五十四條：航空安全法（Luftsicherheitsgesetz, LuftSiG）

第一百五十四條之一：為聯盟公民和歐洲經濟區成員引入電子身分證法以及修訂身分證明文件法和其他法規的規定(Gesetz zur Einführung

einer Karte für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums mit Funktion zum elektronischen Identitätsnachweis sowie zur Änderung des Personalausweisgesetz und weiterer Vorschriften, eIDKGEG）

第一百五十五條：生效日

附錄五 參考文獻

外文文獻

1. Ana-Maria Brezniceanu, ‘Data Protection Officer - a new profession in public administration?’ (2017) 55 Revista de Științe Politice 80.
2. Article 29 Data Protection Working Party, ‘Opinion 05/2014 on Anonymisation Techniques’ （2014） http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.
3. Benecke /Wagner, Öffnungsklauseln in der Datenschutz-Grundverordnung und das deutsche BDSG- Grenzen und Gestaltungsspielräume für ein nationales Datenschutzrecht, DVBl 10/2016, S.604-608.
4. C.J Bennett and C.D Raab, The Governance of Privacy: Policy Instruments in Global Perspective (Cambridge MA: MIT Press, 2006).
5. CIPL, Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation, November 2016, 14.
6. Dieter Zöllner, Der Datenschutzbeauftragte im Verfassungssystem, 1995, S. 21 ff.
7. ICO, 2016. ‘Overview of the General Data Protection Regulation (GDPR)’. Available at: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/.
8. ICO, Accountability and governance, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-gover

nance/.
9. ICO, Annual report 2017-18, 19 July 2018. Available at: https://ico.org.uk/media/about-the-ico/documents/2259463/annual-report-201718.pdf.
10. ICO, Data protection officers, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/.
11. ICO, Money, Law and Courage: the Varied Roles of the UK Information Commissioner, 15 March 2018. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/03/money-law-and-courage-the-varied-roles-of-the-uk-information-commissioner/.
12. Mark Elliot, Elaine Mackey Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework, UKAN, 2016.
13. Peter Carey (2018), Data Protection: A Practical Guide to UK and EU Law, Fifth Edition, OUP.
14. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
15. Benecke /Wagner, Öffnungsklauseln in der Datenschutz-Grundverordnung und das deutsche BDSG- Grenzen und Gestaltungsspielräume für ein nationales Datenschutzrecht, DVBl 10/2016.
16. Dieter Zöllner, Der Datenschutzbeauftragte im Verfassungssystem, 1995.

17. Eßer/Kramer/v. Lewinski(Hrsg.), DSGVO BDSG Kommentar, 6. Auflage, 2018.
18. Jotzo,Florian, Der Schutz personenbezogener Daten in der Cloud, 2013.
19. Kruse Julia, Der öffentlich-rechtliche Beauftragte, 2007.
20. Kühling/Buchner, DS-GVO, BDSG Kommentar, 2. Auflage, 2018.
21. Kühling/Martini, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? EuZW 12/2016.
22. Kühling/Seidel/Sivridis, Datenschutzrecht, 3. Aufl., 2015.
23. Schantz/Wolff, Das neue Datenschutzrecht, 2017.
24. Simits, Spiros(Hrsg.), Bundesdatenschutzgesetz, 8. Auflage, 2014, Einleitung.
25. Sydow(Hrsg.), Bundesdatenschutzgesetz, 2019.
26. Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, 5. Aufl., 2014.
27. Scholz, Kommentar zum BDSG, 8. Aufl., 2014.
28. Voßhoff, Andrea/ Hermerschmidt, Sven, Endlich! - Was bringt uns die Datenschutz-Grundverordnung, PinG 2/2016.
29. Wohlgemuth/Gerloff, Datenschutz, 3. Aufl., 2005.
30. Wolff/Brink, Datenschutz in Bund und Ländern, München: C.H. BecK, 2013.

中文文獻

1. 蔡宗珍，憲法人格權之保障及其界限-兼論網路人格權保護之憲法挑戰，第 9 屆憲法解釋之理論與實務學術研討會，中央研究院法律學研究所，2013 年 6 月。
2. 李寧修，預防性通信資料存取之憲法界限-以歐盟儲備性資料存取

指令（2006/24/EG）之發展為借鏡，興大法學，17 期，2015 年 5 月。

3. 李寧修，個人資料合理利用模式之探析：以健康資料之學術研究為例，臺大法學論叢，49 卷 1 期，2020 年 3 月。
4. 李振瑋、江耀國，英國資料保護法中資料所有人權利之研究 – 兼論我國個資法之相關規範及案例，中原財經法學，第 24 期，2010 年 6 月。
5. 翁逸泓、廖福特，私生活權利：探索歐洲，反思台灣，台北：新學林出版，2014 年 12 月。
6. 達文西個資暨高科技法律事務所，國家發展委員會 106 年度「個人資料保護專責機關與資料在地化之法制研究」委託研究計畫結案報告，國家發展委員會，2018 年 5 月 15 日。
7. 劉靜怡編，人工智慧相關法律議題芻議，元照出版，2018 年 11 月。

附錄六 期中報告審查會會議紀錄

「歐盟國家個人資料保護法制因應 GDPR 施行之調適-以德國與英國為例」委託研究計畫期中報告審查會會議紀錄

壹、會議時間：108年11月29日（星期五）下午2時

貳、會議地點：本會法制協調中心3樓會議室

參、主席：林參事志憲(劉副主任美琇代理)

肆、出（列）席人員：(詳後附名單)　　紀錄：陳韻如

伍、主席致詞：(略)

陸、報告事項：世新大學（略）

柒、發言要點：(依發言順序排列)

一、 東海大學法律學院范姜教授真嫩

(一)名詞解釋之部分(例如：accountability、compliance)，建議翻譯使用較容易理解的文字，或在翻譯後面加上原文；另建議期末報告在各小節加上標題，以利閱讀。

(二)德國與英國對於醫療資訊是否有特別規定，或是僅於個人資料保護法中規定，因該等資料涉及公共利益、個人隱私甚深，建議併予說明。

(三)報告第 52 頁最後一段敘及英國國內對 GDPR 之執行層面區分兩個不同機關之職責一節， IC (Information Commissioner)與 ICO (Information Commissioner's Office)之間，是何種關係？層級或隸屬關係？有關地方的 DPO 如何進行指派、其與 ICO 之關聯性為何？請研究團隊說明。

二、 政治大學法學院劉教授定基

(一)特種個資目的外利用或是特種個資利用的合法事由，於英國與德國之個資法及 GDPR 是否係採雙重適用(疊加適用)？如是，其理由為何？建議研究團隊就此部分補充於期末報告，並與我國個資法做比較，俾提供委託機關將來在修法時參考。

(二)有關特殊監管領域部分，報告第 28 頁說明德國係將廣電(及宗教，但宗教於我國應無類似特殊性，故可暫不論)列為特殊監管領域；而英國部分似全部歸由 ICO 監管。二國不同作法背後之考量因素為何？建議於期末報告稍加分析，並提出對我國之修法建議(例如：對於通訊傳播、金融等領域，有無採取特殊監理之必要)。

(三)關於監管機關中央與地方權限之劃分，英國地方政府的 DPO 雖可作為與 ICO 之間的溝通橋樑，但僅監管其所屬機關個人資料保護事項，似乎沒有對非公務機關進行「監理」，與德國監察官不同，建議期末報告對德國及英國的現況提出比較，並對我國提出修法建議。

(四)研究報告已對德國與英國個資法主要條文提出翻譯及比較分析，建議於期末報告中針對未來個資法修正的關鍵問題，例如：主管機關權限、去識別化的規範、可攜權與被遺忘權等，提出具體修正條文草案(當然，如研究結論認為不需增訂特定權利，亦可建議不修法)。

三、東吳大學法律系葉教授奇鑫

德國為因應 GDPR，修正了相當多之法律，建議將修正之重要法律名稱(非個別條文)翻譯出來，作為未來修法之參考；英國的部分，建議將 ICO 年度報告(annual report)中關於調適的方向與實際作為(如人力增加)等整理列出，以增加報告之完整性。

四、法制協調中心

(一)建議於期末報告將德國、英國個資法的重要條文譯為中文，整理至附錄，以符契約需求及便於查閱。

(二)建議於期末報告時調整報告架構，先介紹 GDPR 再分述德國、英國個資法,避免各別於德國與英國法制分析均重複敘述 GDPR 之相同規定。

五、研究團隊回應

(一) 中國文化大學法律學系李教授寧修

1. 感謝審查委員所提供之意見，用字格式部分研究團隊將再進行調整及修正。

2. 醫療資訊部分，GDPR 及德國個資法雖均有相對應的要求，但係屬框架式規範，故大多會制定特別法為進一步規範。由於 GDPR 有授權各會員國針對健康資料部分透過內國法進行規範，如德國個資法在自動化決定之部分，即有開放可以處理健康資料，但其同時亦相當強調當事人知情同意之要件，而於此前提下，即相對限縮處理之可能性。

3. 德國個資法對於 DPO 相關規定部分，將於期末報告時，再為增補。

4. 針對特種個資目的外處理要件的部分，德國個資法上係要求先符合一般個資目的外處理要件，再配合 GDPR 或德國個資法對特種個資目的外處理之規範。這樣的規範體系除了避免重複性規定的立法技術層面考量外，研究團隊也會再為探究此一立法模式者是否有其他的考量。

5. 德國法上針對特殊領域之監管，在電信這個領域，原則上電信法之規範將優先個資法適用，但是針對德國境內最大電信公司 Deutsche Telekom(類似我國中華電信)，就其個資處理，

則係交由聯邦個資保護暨資訊自由監察官進行監管。由於GDPR 對於特殊領域之監管亦給予各會員國一定空間，而德國目前係就廣電及宗教與教會兩大部分，分設監察官為監督管理。

6. 委員建議提供修法建議部分，德國個資法就可攜權並未有規範，即依據 GDPR 之規範行之，此部分可能就不會再為比較及整理。

7. 有關德國個資法因應 GDPR 第 2 次修法之部分，由於德國採取包裹式修法，修法時會針對所有可能涉及的條文進行一次性的修正，但是目前觀察此次修正中，與德國個資法有關的修正於第 12 條，修正之內容並不多。而其他修正之法律，如涉及警察法、刑事司法、社會法等相關部分，因非本次研究之重心，故僅會就修法歷程及重點做大致上之說明，討論仍是會著重於個資法。

(二) 世新大學法律學院翁教授逸泓

1. 「Accountability」翻譯為「責信」是因其重點在於信任度，所以將信這個字放進來，不過關於此部分將再做相關用字調整與修正。

2. 在英國關於醫療資訊的部分，由於英國沒有特別的規範，而英國特殊的部分是其 ICO 的能量強大，例如：電信方面有處理 PECR(隱私暨電子通訊規則，Privacy and Electronic Communication Regulations)的規範，也有自己的規則(regulation)可以適用，只有在很特別的地方會切割開來。醫療資訊的部分，ICO 做了一些要求的審查流程以及標準契約版本的內容，舉例而言：健保資料庫(NHS digital)的資料，若要供商業應用時，則須符合商業標準應用的要求，ICO 提供

標準版本契約得以進行修改，這應該是之後專責個資保護之主管機關要做的事情，英國的部分目前是如此操作，但是必須要注意的是英國得以如此進行，是因為英國主管機關 ICO 的龐大且人力正在急速地擴張。

3. 英國法上比較像是中央集權、一條鞭的概念，地方政府機關有無法處理的問題時，會與 ICO 開會諮詢，未來我國也可以將此納入考量。ICO 會指導設置 DPO 的時候需注意哪些事情，應如何指派、職責是什麼、如何與 ICO 聯繫，並定期有教育訓練可以參加，如何更換人員，以及應該保有如何程度的獨立性，且 DPO 會是聯絡的窗口，未來有任何事情只要基於 DPO 的獨立性可以主動與 ICO 通報，反之若是 ICO 發現時，也會請 DPO 先行了解，作為一個聯繫的功能。類似於我國目前消費者保護制度，就現行臺灣制度是地方也會有消保官，理論上與地方政府也並不是這麼的具有從屬性。可是畢竟不太一樣，只是一個類似的想法，我國若要以此為借鏡，或許有某種程度上的可能性。

4. 雙重適用之問題上研究的想法是，要符合特種個資的利用必定會先符合一般性資料的運用，在邏輯上本來就是應該要符合前半段所謂的法定原則才會落入特殊的規範，若逐一規定的話就會像 DPA 2018 的 Schedule 1 以及 Schedule 8 一樣冗長，例如：報告第 74 頁以下，公共利益內容為何，其實裡面多數的構成要件都很雷同，諸如把必要性、合法性又都再寫了一次...等等。除了合法性與必要性之外，還需具備其他的要件，其實多為輔導建議，因此針對於未來的修法建議上，不建議將條文書寫成如此繁雜的內容。若要採行此種方式，建議可將條文轉換為「除...還需...」之文字。

5. 被遺忘權與可攜權有相似的問題，因 GDPR 在壓力團體遊說下修改過多次的版本，會引起爭議可想而知，因此英國在立法時避開了這個問題，以 GDPR 之規定為主，而脫歐之後的規範則寫在 DPA2018，多承襲 GDPR 的內文；被遺忘權相較可攜權疑義較少，而因可攜權會供給產業上之運用，衡量於大公司與新創公司之間不同的需要，政策的選擇將會影響此部分的寬鬆程度。

捌、會議結論：

(一) 請研究團隊將委員所提相關意見納入後續期末報告修正。

(二) 對於本計畫就主管機關權限、去識別化規範、可攜權與被遺忘權等議題，請研究團隊在研究德國與英國因應 GDPR 調適其個資法制時，除依契約書比較兩國與我國個資法之分析外，並請就我國後續修法方向與條文提出建議。

玖、散會（下午3時35分）

附錄七 期中審查意見回應說明

歐盟國家個人資料保護法制因應 GDPR 施行之調適-以德國與英國為例

期中審查意見回應說明

編號	委員	建議	研究團隊回應
1	范姜 教授 真嫩	名詞解釋之部分(例如：accountability、compliance)，建議翻譯使用較容易理解的文字，或在翻譯後面加上原文；另建議期末報告在各小節加上標題，以利閱讀。	感謝審查人建議，本研究修正與新增說明： 1. 名詞部分統一翻譯為「課責原則(Accountability Principle)」。 2. 將標題予以精細化，各小節均新增標題。
2		德國與英國對於醫療資訊是否有特別規定，或是僅於個人資料保護法中規定，因該等資料涉及公共利益、個人隱私甚深，建議併予說明。	關於醫療資訊之規範，分別於審查報告中補充說明英國及德國之規範情形： 1. 英國部分：尚無關於醫療之個資保護特殊規定，均回歸至個資法，而實務上多以法院判決對特殊情況調適。 2. 德國部分：關於醫療資訊之規範，並未有專法，而係散見於聯邦及各邦之法律中，補充說明於頁 129-130 中。
3		報告第 52 頁最後一段敘及英國國內對 GDPR 之執行層面區分兩個不同機關之職責一節， IC (Information Commissioner)與 ICO (Information Commissioner’ s Office)之間，是何種關係？層級或隸屬關	關於此二機關之不同職責，本報告釐清後說明於頁 11： 1. 政府部門確保 GDPR 於英國要求之適足性的部會係為英國文化、媒體與運動部(Department

編號	委員	建議	研究團隊回應
		係？有關地方的 DPO 如何進行指派、其與 ICO 之關聯性為何？請研究團隊說明。	for Digital, Culture, Media and Sport, DCMS)，且 **DCMS 也負責制定英國資料保護之立法**，但並不執行 DPA 2018 之實際施行； 2. 相對地，英國資訊委員（辦公室）(The Information Commissioner's Office, ICO)職責之一即在落實執行 GDPR，其權力包括（關於個資）犯罪調查與罰鍰等，並提供企業與人民團體與政府機關部會(包含地方政府)對於如何適應 GDPR 之指引。
4	劉教授定基	特種個資目的外利用或是特種個資利用的合法事由，於英國與德國之個資法及 GDPR 是否係採雙重適用(疊加適用)？如是，其理由為何？建議研究團隊就此部分補充於期末報告，並與我國個資法做比較，俾提供委託機關將來在修法時參考。	感謝審查人建議，將於期末審查會議後修改本報告時，新增以下段落於適當段落： 1. 英國部分： 通常理解 GDPR 最常出現的問題之一在於解讀例外豁免得對個資當事人之個資處理條件時，僅考量該等例外豁免得處理個資之特別要件，例如 GDPR 第 9 條第 2 款或第

編號	委員	建議	研究團隊回應
			22 條第 2 項之規定等，而忽略了 GDPR 之規範在處理**所有的**個資時，均需要符合第 5 條之個資保護之核心原則（如個資目的性原則、最小化原則、合法、公平、透明、正確、限期原則等），並有第 6 條適法之基礎等一般要件。細言之，基於個資保護必須先滿足核心原則，**所有的**個資處理都須符合各項原則方得為處理。但在特種資料範疇內為個資處理時，除了在**邏輯上特種個資之處理當然要先符合所有個資處理之核心原則**外，又區分為特種個資之一般處理以及特種個資之自動化做成決策而各有例外豁免要件。[315]於特種個資之一般處理情況時，須符合 GDPR 第 9 條第 2 項(a)至(i)之豁免要件其一，方得例外地進行一般處理；至於特種個資之自動化做成決策之情狀，則

[315] WP 29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01).

編號	委員	建議	研究團隊回應
			依 GDPR 第 22 條第 4 項之規定，更嚴格限縮至僅在第 9 條第 2 項(a)與(g)項的兩種例外豁免條件滿足之時，方得為之。 2. 德國部分： 德國個資法就特種個資之目的外處理，確實係採用一般個資目的外處理要件，加上 GDPR 或德國個資法就特種個資之處理要件為雙重適用，此與 GDPR、我國個資法與舊德國個資法之規範模式均有所不同。就此，應係立法技術上避免重複規範而採行之作法。
5		有關特殊監管領域部分，報告第 28 頁說明德國係將廣電(及宗教，但宗教於我國應無類似特殊性，故可暫不論)列為特殊監管領域；而英國部分似全部歸由 ICO 監管。二國不同作法背後之考量因素為何？建議於期末報告稍加分析，並提出對我國之修法建議(例如：對於通訊傳播、金融等領域，有無採取特殊監理之必要)。	1. 由於 GDPR 就廣電部分有授權各國得採行不同作法，故德國於邦之層次，有依據邦之個人資料保護法就廣電部分另設立廣電個人資料保護監察官者。由於德國不論聯邦或各邦之個人資料保護監管機關均係採首長制，考量監管領域之需求及專業性，即有設置多個監管機關之作法。而對於我國是否有依據領域分

編號	委員	建議	研究團隊回應
			別監管之必要，在獨立、專責之前提下，首先可考慮是否屬 GDPR 有授權之領域，例如設置金融領域特別監管的可能性即可能受到限縮；其次，則為我國監管機關欲採行之體制為何（單一式或分散式、首長制或合議制），進行綜合考量。 2. 英國關於通訊傳播與隱私之規定為 PECR，對應歐盟 ePrivacy Directive，與 GDPR 均為 ICO 監管。本報告於頁 179 建議如下： 至若因應數位匯流時代之法律規範，基於我國已有通訊傳播委員會(NCC)之獨立專責機關，地位對應英國之通訊辦公室(Office of Communications, Ofcom)。然，「數位通訊傳播法」以及「電信法」修法之相關草案雖已送入行政院會，但等待多時仍未見具體審議時間。而 NCC 計畫草擬之 OTT-TV 對應法規「網際

編號	委員	建議	研究團隊回應
			網路視聽服務法」也仍未見具體草案輪廓，則對應個資保護交錯之相關指引，當然也難尋蹤跡。基於此，個資法未來修正時如仍以關於個資保護之普通基準法之定位規範，則在須靈活變通的數位匯流時代通訊傳播法中是否有針對特定類型資料或者特定目的利用，仍得解釋為有增訂特別規定的空間。
6		關於監管機關中央與地方權限之劃分，英國地方政府的 DPO 雖可作為與 ICO 之間的溝通橋樑，但僅監管其所屬機關個人資料保護事項，似乎沒有對非公務機關進行「監理」，與德國監察官不同，建議期末報告對德國及英國的現況提出比較，並對我國提出修法建議。	1. 德國邦之個人資料保護監察官，亦為德國個資法中所稱監督機關，其負責監管非公務單位其所屬公務單位。而於其所監理之公務及非公務單位中，亦依據德國個資法第 5 條及第 38 條之要求，任命個人資料保護監察長。 2. 英國之 ICO 採取較為中央集權之制度，對於非公務機關例如中小型企業之需求採取所謂**一站式服務**，由 ICO 直接監理。與德國之聯邦制度不同。參頁 13-14：

編號	委員	建議	研究團隊回應
			（1）對 DPO 之支持 ICO 認為 GDPR 與 DPA 2018 對 DPO 賦予重要之責任，尤其是在新的個資保護規範架構下，DPO 對於促使各機構組織快速適應新法，有著重要角色。 據此，ICO 每年均針對 DPO 召開在實踐個資保護政策上的研討會，並頒發相關獎項鼓勵傑出 DPO，也趁機對其宣達政策。 （2）對中小企業(SMEs)之支持 除了前述有 DPO 的組織以外，ICO 也充分理解小型組織要符合 GDPR 和 DPA 2018 並非易事，尤其是對於個體交易者而言，更顯其困難。為此，ICO 提供了一套資源、支持和指南，專門針對個體交易者和小型組織的需求，包括可能的操作選項和清單，社群媒體平台和常見問題解答。ICO 也對此提供了專門的求助熱線和即時聊天服務，以提供進一步的幫助和建議，並舉行了由數百家中小企業參加的諮詢會議。

編號	委員	建議	研究團隊回應
			除了這些服務以外，ICO 目前正在探索為中小企業建立「一站式服務」，以匯集各個監管團隊的專業知識來幫助 ICO 為所有中小企業提供支持-尤其是對於那些沒有能力或沒有義務維護專用內部合規資源的中小企業。
7		研究報告已對德國與英國個資法主要條文提出翻譯及比較分析，建議於期末報告中針對未來個資法修正的關鍵問題，例如：主管機關權限、去識別化的規範、可攜權與被遺忘權等，提出具體修正條文草案(當然，如研究結論認為不需增訂特定權利，亦可建議不修法)。	參見附錄一、二。
8	葉教授奇鑫	德國為因應 GDPR，修正了相當多之法律，建議將修正之重要法律名稱(非個別條文)翻譯出來，作為未來修法之參考；英國的部分，建議將 ICO 年度報告(annual report)中關於調適的方向與實際作為(如人力增加)等整理列出，以增加報告之完整性。	1. 針對德國 2019 年 11 月第二次因應歐盟 GDPR 及歐盟第 2016/680 指令所為修法中，一併修改之 154 部法規名稱，將於會後以附錄形式附加於審查報告末。 2. 感謝審查人具體建議，本報告將此部分新增於頁 12-16。
9	法制協調中心	建議於期末報告將德國、英國個資法的重要條文譯為中文，	於審查報告末以附件形式節錄德國個資法及英國

編號	委員	建議	研究團隊回應
		整理至附錄，以符契約需求及便於查閱。	2018 年資料保護法相關條文翻譯，請見附錄一、二。
10		建議於期末報告時調整報告架構，先介紹 GDPR 再分述德國、英國個資法，避免各別於德國與英國法制分析均重複敘述 GDPR 之相同規定。	基於避免在兩國之相關分析時重複敘述 GDPR 相同規定，本研究將德國、英國之順序對調，在論述英國之部分，在大多數分析中採取先說明 GDPR 規範，再分析英國調適之情況。 於德國部分，則除非有前述英國部分中關於 GDPR 為論述完整者，否則主要焦點集中說明英德國調適之情況，GDPR 部分不再說明。

附錄八 期末報告審查會會議紀錄

「歐盟國家個人資料保護法制因應 GDPR 施行之調適-以德國與英國為例」委託研究計畫期末報告審查會會議紀錄

壹、會議時間：109年5月21日（星期四）上午8時30分

貳、會議地點：本會法制協調中心3樓會議室

參、主席：林參事志憲

肆、出（列）席人員：(詳後附名單)　　紀錄：陳韻如

伍、主席致詞：(略)

陸、報告事項：世新大學（略）

柒、發言要點：(依發言順序排列)

一、 東海大學法律學院范姜教授真媺

(一) 建議修改報告中之錯漏字，相同之外語建議使用相同之中譯(例如：right to object)，易混淆之用語，建議增加註腳解釋，第 71 頁「Request for personal data」圖表建議翻譯為中文，第 153 頁以下有關德國法於計分及支付能力查詢之經濟交易保護，建議先解釋「計分」，再作後續論述。

(二) 去識別化部分，在德國法與英國法，假名化與匿名化之區別方式，並未在報告中看到詳細的定義，是否比照歐盟的標準；是否將「去識別化」認定為資安的問題，而無需對匿名化及假名化的程序要件進行規範；而在德國法與英國法對去識別化的作法為何？判斷標準為何、以誰為判斷標準？

(三) 德國與英國之獨立監管機關顯然為兩個不相同的制度，而我國應該要怎麼做，考量我國人口數與領土範圍，若採德國設立多個監管機關的方式或許會造成人員與經費上的負擔，若採英國的中央集中監管之方式或許比較適合，則地方政府應如何因應？地方政府是否須設置DPO，是否如同現行消費者保護官的職位，

若地方設置了 DPO 的職位，其與中央之權限上如何劃分？聯繫管道為何？有無指揮監督關係？

(四) 英國的 DPO 與中央 ICO 的關係為何？DPO 可外聘自然人或法人擔任，於組織內之公務員擔任 DPO 與委外的 DPO 兩者之責任、職務忠誠度上是否有落差？利益衝突應該如何處理？英國法如何規定？

(五) 勞工保護的部分，因為勞資雙方有資力不對等的情況，而資方保有許多勞工的個資，以我國現行的個人資料保護法是否足以保障勞工的權益？也許可以借鏡參考日本，是由勞動省訂定相關指引，整合勞工個資保護的問題。

二、 東吳大學法學院葉教授奇鑫

(一) 研究團隊針對期中報告審查意見第 8 點之回應，翻譯並整理「德國 2019 年 11 月因應 GDPR 第二次修法修正法規名稱」，是非常有價值的參考文件，建議置於報告附件。

(二) 第 200 頁提及建議特殊處理情形於個資法中為框架性規定，有助於規範之一致性及對個人資料保護之完整性一節，我的看法是很多規定應該訂在各部會主管的法規較妥適，例如勞動法規，未來若有中央獨立監管機關，建議訂定框架式規定，再由各主管機關於該框架下訂定詳細規定；我國畢竟只需滿足 GDPR 的適足性認定，不像英國、德國或其他歐洲國家必須直接符合 GDPR 規定，假設臺灣處於歐盟的框架下，恐怕也是需要修改許多法條，但這或許也是我們未來的方向。

(三) 第 71 頁之流程圖與一般流程圖畫法稍有不同，建議再確認一下，若是 ICO 所發布之原件則不需修改。

三、 政治大學法學院劉教授定基

(一) 建議英翻中之語意再稍微調整、梳理，以中文的語法翻譯，並以「意譯」之方式以利閱讀。例如：第 35 頁「DPA 2018 之立法規範模式不在於過度嚴格地緊縮特種個資絕對禁止處理之原則」，意思究竟是「放寬」還是「更緊縮」較難理解；第 39 頁 C 款、第 77 頁個資排除事由等，較近似直譯，好處是忠於原文，但可能影響全文的可讀性。

(二) 建議在結論章節，將討論編排順序重新調整，同一議題或同一標題下，分別就英國、德國論述，再以共通性的觀察或結論、統整歸納、並以對我國的建議作為小結。

(三) 承上，結論部分是否能有共同或統一的見解，例如特種個資之利用，借鏡英國與德國落實 GDPR 的經驗，並非如同大家所想的有越來越嚴格的趨勢，報告在英國、德國部分分別有提到此一觀察，但結論部分沒有，僅表示德國法部分看來似有放寬的跡象；在去識別化方面，雖然有意見認為我國目前對去識別化的定義不清楚，但若從德國與英國的實踐來看，再進一步明確化「去識別」的定義確實是有難度的事情，因此我國未來修法是否要訂定去識別化的規定，可以參考這兩個國家及其他國家(例如日本)之作法，作成建議。

(四) 特殊處理情形方面，觀察臺灣現況，個別法律會規定「依個人資料保護法規定辦理」，指回適用個資法；換言之，當其他法規利用到個資且要訂定個資蒐集、處理、利用辦法時，各部會都會說按照個資法規定處理。與德國法或英國法比較，這是跟我國明顯不一樣的地方，結論可能會有兩個，其一：直接於個資法訂定框架規定；其二：個別領域因其特殊性，應針對各個不同的法規進行修正；由各機關負責訂定法規及執行，但這與單一監管機關的制度是否會有矛盾？在德國法部分較為特殊，

較不會產生這類問題，假設我國未來成立個人資料保護委員會，勞動部訂定涉及勞工個資之相關法規，應以誰的意見為主？各主管機關與中央監管機關權限有衝突時該如何處理？建議研究團隊可以稍作補充。

四、 法制協調中心

(一) 依照 GDPR 規定，監管機關須具獨立性，且有人事、預算、裁罰等權限，爰本報告將 DPO 放在監管機關章節下似有未妥，且可能誤解未來我國設置 DPO 即符合歐盟監管機關之要求，爰建議將 DPO 移列至後面單獨章節討論。

(二) 本計畫需求書所列第 2 個研究議題為「個資特定目的外利用之要件」，英國法僅分析特種個資而未分析一般個資之目的外利用要件，建議於英國部分予以補充。

(三) 當事人權利的部分，德國法部分係將 GDPR 當事人查詢、告知、刪除等相關權利，就 GDPR 授權各國得為限縮規定部分逐一分析；惟英國法部分僅針對兒童權利進行分析，建議參照德國法將 GDPR 相關當事人權利於英國法予以限縮部分逐一分析。

(四) 德國、英國與我國個資法的比較，建議將本研究 6 項議題逐一列表分析較為清楚，或是如同劉老師的建議以議題式的編排做分析。

(五) 第 50-51 頁，英國法關於去識別化資料於政府資訊公開、開放資料如何適用之部分，因報告僅簡單帶過，是否可以請研究團隊就這個部分補充說明。

(六) 第 94 頁最後一行「可進行單純自動化決策的三種例外情況簡單舉例」，後面未說明例外狀況為哪三種、第 174 頁最後一段提及巨量資料再利用可區分三種不同情狀，後面也未說明哪三種

情狀，建議引註說明；第 212 頁德國個資法第 23 條，第一段應為該條的第 6 點。

五、 研究團隊回應

(一) 世新大學法律學院翁教授逸泓

1. 針對審查委員提出的自動化做成決策，究是防禦權還是拒絕權的問題，就體系解釋來說會解釋為拒絕權，而在閱讀文獻時，有些會解釋成調查權，造成不同的見解。拒絕權分成兩段，首先，根本不讓機器自動化處理個資；若萬一沒有在這邊行使拒絕權，讓機器自動化處理個資後，仍然有拒絕權，可以拒絕自動化所做成的決策，某種程度上可以說是防禦權，但是拒絕權還是防禦權會再加以討論。

2. 匿名化與假名化的差別，大致上的區別標準是在判定到底哪一種是屬於可以接受的資料再識別風險，係科學技術、自然技術上再識別的風險與當代的科技可以接受容忍到何種程度，程度上來說會是資安的問題，但常常會有人把個資保護與資安混為一談，我的想法是資安的保護範圍其實沒有個資保護範圍來得這麼大，就種類來說資安也只是個資保護的一種類型。因此，若在資安上可以處理到當代技術無法破解，且資安在一定程度之上、科學的再識別風險極低的話，不妨把它視為匿名化，但在法制、組織上需訂定配套措施。

3. 英國 ICO 採中央集權制，地方設立 DPO 的功能就是連繫與控管內部，發生任何事情進行通報，亦即應變與內控的窗口，而實際操作仍由中央機關執行。

4. 法人擔任 DPO 之責任落差與利益衝突之規範，第 32 頁以下有相關說明，例如：DPO 對於利益衝突該如何處理，若是公務機關內部的成員作為 DPO，理論上應該相較其他人更熟悉

組織，因此資料治理方面要求會高一些；若 DPO 是機關編制內的人員仍有一定程度上的機關從屬性，因此是具有豁免權，不會因為履行 DPO 職務而受罰，但是會特別要求有關利益衝突的問題。

5. 特殊處理情形是否在個資法做框架規定，英國目前的處理方式是由 ICO 作出準則，請各機關按照準則訂定規定，規定只要不違反這個準則即可。相當程度上 ICO 還是會有他的角色，提供準則、細部指引供各機關參考。

6. GDPR 的 G 係指 General，是一般性規定的意思，即便以歐盟層級來看，也包含了許多不同領域，但我國目前只侷限在 GDPR 裡面的項目，而忽略外部領域之項目，以犯罪偵查為例，我國於通保法規定，但只要與隱私有相關的，英國仍是由 ICO 做出準則，而在各個機關制定法律時就隱私的部分需要符合 ICO 程度的規定；並且 ICO 會對各機關所修正的法律提供意見、指導。

7. 有關各機關立法時又指回適用個資法，若有中央監管機關，遇到此情形時，可以告訴相關機關應適用哪些準則，若需立法時也是依準則訂定相關規定而不是指回適用個資法，這也是中央監管機關存在的必要。

(二) 中國文化大學法律學系李教授寧修

1. 關於三位審查委員及法制協調中心所提及之格式、錯漏字及德文翻譯等部分，會於後續期末報告修正之時通篇處理並改正。

2. 針對范姜老師所提及之「單位」一詞，選譯「單位」，一方面係因德國法上針對這個詞彙，代表較上位之概念，包含機關、公法社團及財團、公營造物及行政法人等，都可以被涵

蓋其下。另一方面，則是參考法務部先前翻譯德國聯邦個人資料保護法時所使用之用語。此用語我國法制上也許會被誤解為內部單位，故後續修改時，會再思考是否有其他更好之用語可以取代；若無較佳用語可以取代時，將以註腳之方式予以解釋及說明其所代表之意涵。

3. 針對匿名及假名化定義部分，舊德國個資法時代係有針對假名化進行定義；但在 GDPR 施行後，新修正德國個資法便刪除了假名化之定義，改為遵循 GDPR 對於匿名及假名化之定義。

4. 關於監管機關之部分，考量個資屬於全國一致性事項，應該由中央統一負責為妥。至於是否應適度委由地方自治團體或是設置 DPO 等，若是採取此種分散式管理制度，此時應當考量之問題為中央與地方間聯繫之部分。參考德國聯邦及邦監督機關之運作，除以此聯繫、溝通作為法定任務外，另外會定期舉行會議，針對個資問題予以討論，建立具一致性之個資保護標準。

5. 針對特殊處理情形是否有必要特別立法規範及立法後是否會有特別法優於普通法適用問題之部分，首先必須說明的是，我國目前針對特殊處理情形並無類似規範，若有意立法規範，就德國法之規範模式而言，其係以 GDPR 之規範作為基礎，再以特別法之規範來放寬或提升規範強度。因此，若想提升個資合理使用，在我國個資法內透過特殊處理情形之規定為鬆綁，係有其參考之價值；若想以特別法來規範亦無不可，惟應注意的是，個資之合理使用判斷常常須導入必要性或比例原則去作法益權衡，但特別法因並非如個資法係以「保護個資當事人權利」為其立法目的，亦未必會關注個資法上相關原則，例如：目的拘束原則、透明性原則等，此時在特別

法規範下作利益權衡，恐會產生對當事人權利保障不甚周延之虞。故若能在個資法內為框架性或基準性立法的話，也許能確保特別法對於當事人權利部分有較為完整之考量。

6. 由於德國法係採取包裹式立法，故針對 GDPR 施行一事，其以立法之方式進行全面性法規盤點並加以修正。採取此種立法模式，或能有效避免不同法規間立法歧異之問題；惟此種立法模式並非我國所採。

捌、會議結論：

感謝與會者今日參與並提供寶貴意見，請研究團隊依委員及本會意見修正期末報告內容後提送本會。

玖、散會（上午10時30分）

附錄九 期末報告審查會會議紀錄

歐盟國家個人資料保護法制因應 GDPR 施行之調適-以德國與英國為例

期末審查意見回應說明

編號	委員	建議	研究團隊回應	頁次
1	范姜教授真媺	建議修改報告中之錯漏字，相同之外語建議使用相同之中譯(例如：right to object)，易混淆之用語，建議增加註腳解釋，第 71 頁「Request for personal data」圖表建議翻譯為中文，第 153 頁以下有關德國法於計分及支付能力查詢之經濟交易保護，建議先解釋「計分」，再作後續論述。	1. 修正該處錯字。 2. 調整論述並增加註腳： 就此處 right to object 之相關權利言，在解釋上向來有關於此處係為「禁止」傾向保護個資當事人利益，或是「有權反對」之防禦，而傾向維護個資控管者之權利，一向有所爭論。本研究在英國部分作者較傾向前者，本研究在德國部分相關介紹時，則以抵禦之權利說明。事實上在學說上仍未有定論，相關之辯論詳參：Bygrave, Lee Andrew (2020). Article 22: Automated individual decision-making, including profiling, In Christopher Kuner; Lee Andrew Bygrave & Christopher Docksey (ed.), The EU General Data Protection Regulation (GDPR): A Commentary, 530-532.基於本研究雖盡量希望能統整論述，惟為避免與個別作者之學說一貫性論述發生矛盾，仍採分別立場，並以此為註。 3. Request for personal data 圖表	58

編號	委員	建議	研究團隊回應	頁次
			已翻譯為中文。 4. 針對德國個資法第 31 條所稱「計分（Scoring）」，補充其定義之說明。	48 112
2		去識別化部分，在德國法與英國法，假名化與匿名化之區別方式，並未在報告中看到詳細的定義，是否比照歐盟的標準；是否將「去識別化」認定為資安的問題，而無需對匿名化及假名化的程序要件進行規範；而在德國法與英國法對去識別化的作法為何？判斷標準為何、以誰為判斷標準？	增加文字： 須注意者，由於該報告出版年係在 GDPR 正式上路之前，因此在文字上仍有關於匿名/假名混淆之情況。例如在 Anonymisation: managing data protection risk code of practice 之報告版本指引中即指出： …我們使用廣泛的術語「匿名化(anonymisation)」來涵蓋可用於將個人資料轉換為匿名資料的各種技術。例如，我們區分了用於產生集合資訊(aggregated information)的匿名化技術以及假名化(pseudonymisation)，即以個人為單位而產生匿名資料之技術。… 那麼，在 GDPR 修法之後，英國又如何區分匿名與假名？原則上依據 ICO 之區分，仍遵照 GDPR 之規範加以區分。 在匿名方面，ICO 一樣認為這意味著已匿名的個人資料不受	36-39

編號	委員	建議	研究團隊回應	頁次
			GDPR 約束。因此，匿名化可以成為限制風險以及為個資當事人帶來益處，也因此 ICO 鼓勵在任何可能的地方對個資進行匿名處理。同時，依照 GDPR 之解釋，ICO 也提醒在嘗試匿名處理資料人數時，應謹慎為之。實際操作上，雖然很多組織或個資控管人通常稱個人資料集為「匿名」時，事實上並非如此。為了根據 GDPR 進行真正的匿名處理，ICO 認為必須刪除個人資料中足夠多的元素，這意味著無法再識別該個人。相對地，如果可以隨時使用任何合理可用的方法來重新辨識資料所指向的個人，則該資料將不會被有效匿名，而只會被假名化。這意味著，儘管個資控管人嘗試進行匿名化而逸脫於 GDPR 之範圍，但事實上其仍繼續處理個人資料而為規管範圍。 因此無論在定義上、程序要件上，及相關判斷標準上，在未有進一步的更新指引前，均依照 GDPR 之標準與解釋。 不過即便是 GDPR 已然生效且將匿名與假名兩個概念完全區分，至目前為止 ICO 仍未更新關於匿名/假名化之相關指引，仍建議大眾參照舊有之指引與報告。	

編號	委員	建議	研究團隊回應	頁次
			…最後，關於假名化之流程與操作準則，ADF 報告則將其區分為揭露風險評估與控制（Disclosure Risk Assessment and Control）及影響管理（Impact Management），並分別有複雜的子階段。 另外，針對德國法部分，就去識別化技術之運用，係納入德國個資法第 22 條第 2 項所定「適當特定措施」中予以例示，其中之「假名化」，由於德國個資法中並未加以定義，故即以 GDPR 為準；而「匿名化」之要求，則得見於各別處理個資之要件中，例如：德國個資法第 27 條第 3 項針對基於科學或歷史研究目的以及統計目的處理特種個人資料，即有匿名化之要求。但於不同情況中，究竟應選擇何種去識別化措施，普遍仍認應依據 GDPR 第 35 條進行個資保護影響評估之結果決定之，故對於去識別化應達到之程度，包括方式之選擇及判斷之標準等，德國個資法中似選擇留白，給予個案依實際情況有彈性選擇之空間。	127
3		德國與英國之獨立監管機關顯然為兩個不相同的制度，而我國應該要怎麼做，考量	增加文字： 最後，因為英國之專責監管個資保護機關係具有集權性質之機	19-20

編號	委員	建議	研究團隊回應	頁次
		我國人口數與領土範圍，若採德國設立多個監管機關的方式或許會造成人員與經費上的負擔，若採英國的中央集中監管之方式或許比較適合，則地方政府應如何因應？地方政府是否須設置DPO，是否如同現行消費者保護官的職位，若地方設置了DPO的職位，其與中央之權限上如何劃分？聯繫管道為何？有無指揮監督關係？	關，因此地方政府並無對應專責機關之設置，而依據 DPA 2018 在69條以下規範，中央與地方之公務機關均須有個資保護長(Data Protection Officer, DPO)之設立。DPO 與中央專責監管機關之間之關係，大多為該機關組織關於個資事件之通報窗口，以及教育宣導之用，尚無類似我國地方政府消保官制度之獨立職權，而較傾向作為連動聯繫單位之用，而中央專責機關得對其在一定程度上指揮監督。	
4		英國的DPO與中央ICO的關係為何？DPO 可外聘自然人或法人擔任，於組織內之公務員擔任DPO與委外的DPO兩者之責任、職務忠誠度上是否有落差？利益衝突應該如何處理？英國法如何規定？	關於ICO與DPO之間的關係，原則上英國仍遵行GDPR，例如 GDPR 第39條的諸項法遵責任均須與中央專責監管機關合作。再就道德責任與忠誠義務言，外聘DPO顯然較弱，但仍有契約義務與基本之誠信原則要求，則此處端視契約約定之法律義務標準是否能跟得上道德要求。而利益衝突之部分仍視契約內容決定，詳參本報告英國部分第七節。	78-79
5		勞工保護的部分，因為勞資雙方有資力不對等的情況，而資方保有許多勞工的個資，以我國現行的個人資料保護法是否足以保障勞工的權益？也許可以借鏡參考日	目前我國仍無整合性之勞動領域個資實務規範或指引，僅在個別不同面向（例如勞工健康檢查）上有相關散落之函釋。 為此增補相關文字，說明我國現況：	141-142

編號	委員	建議	研究團隊回應	頁次
		本，是由勞動省訂定相關指引，整合勞工個資保護的問題。	最後，關於勞動保護的部分，目前實務上雇主保有許多勞工的個資，以我國現行的個人資料保護法是否足以保障勞工的權益？雖然比較法上例如英國之DPA也無體系性關於勞動隱私之規範或特別規範，但仍有整合性之指引。反觀目前我國仍無整合性之勞動上個資實務規範或指引，僅在個別不同面向上有相關散落之函釋。 以勞工健康檢查為例，依據勞動部職業衛生安全署解釋，依據「職業安全衛生法」(下稱職安法)第 20 條規定，勞工健康檢查係法律規定雇主應為勞工辦理之項目，其**目的係為選工、配工、職業病預防與職場健康管理**。故該署認為事業單位對其所屬勞工依「勞工健康保護規則」(下稱本規則)所定期限及項目之檢查結果，得依法進行紀錄之保存、處理及利用，尚無需另經勞工書面同意，惟不得逾越前開特定目的範圍，且須依本規則第 21 條第 3 項之規定保障勞工隱私權，以符個資法之規定。而關於應採行之安全衛生措施，也認為基於職業安全衛生設施規則第 324 條之 1 至第 324 條之 3，而合於個資法第 19 條及第 20	

編號	委員	建議	研究團隊回應	頁次
			條法律明文之規定。 然而同一份解釋中也說明似乎勞工得拒絕提供該項健康檢查資料:「**尊重個人隱私**及瞭解勞工不願意接受之原因，再透過勞資協商解決對策；若該勞工仍堅持拒絕，建議留存相關執行紀錄。」，然隨後又另基於實務上常有因健康檢查後續應採取相關健康管理措施而衍生勞資爭議，該署認為職安法施行細則第 41 條已將健康指導及管理措施，增列為安全衛生工作守則內容之一，依職安法第 34 條之規定，勞工對於該守則應切實遵行，建議事業單位亦可將相關之健康管理措施納入該守則規範。 據此，可見實務上即便主管機關之函釋，亦仍有一定之模糊性存在，於勞工隱私權與健康管理措施意欲保障之資方選工、配工、職業病預防與職場健康管理發生競合時，究竟應如何衡平似仍有猶豫。可能的解決之道或許仿照英國由個資專責主管機關發布整合性指引。就目前而言，則不妨借鏡參考日本，由勞動省（部）訂定相關指引，整合勞工個資保護的問題。	
6	葉教授	研究團隊針對期中報告審查	針對德國 2019 年 11 月因應 GDPR	185-193

編號	委員	建議	研究團隊回應	頁次
	奇鑫	意見第 8 點之回應，翻譯並整理「德國 2019 年 11 月因應 GDPR 第二次修法修正法規名稱」，是非常有價值的參考文件，建議置於報告附件。	第二次修法修正法規名稱，將置於報告末之附錄四。	
7		第 200 頁提及建議特殊處理情形於個資法中為框架性規定，有助於規範之一致性及對個人資料保護之完整性一節，我的看法是很多規定應該訂在各部會主管的法規較妥適，例如勞動法規，未來若有中央獨立監管機關，建議訂定框架式規定，再由各主管機關於該框架下訂定詳細規定；我國畢竟只需滿足 GDPR 的適足性認定，不像英國、德國或其他歐洲國家必須直接符合 GDPR 規定，假設臺灣處於歐盟的框架下，恐怕也是需要修改許多法條，但這或許也是我們未來的方向。	感謝審查委員提出建議與看法，本文在前揭關於勞動領域個資保護規範中，新增文字說明，並於委員建議之相關頁數，補充文字：不過，在現階段未有個資保護專責監管機關之情形下，不妨維持由各目的事業主管機關訂定相關指引，以儘速整合各領域相關個資保護之問題。	147
8		第 71 頁之流程圖與一般流程圖畫法稍有不同，建議再確認一下，若是 ICO 所發布之原件則不需修改。	已確認並將之中文化。	48
9	劉教授定基	建議英翻中之語意再稍微調整、梳理，以中文的語法翻譯，並以「意譯」之方式以	感謝委員建議，本研究調整相關譯文： 「英國 DPA 2018 之立法規範模	22、

編號	委員	建議	研究團隊回應	頁次
		利閱讀。例如：第 35 頁「DPA 2018 之立法規範模式不在於過度嚴格地緊縮特種個資絕對禁止處理之原則」，意思究竟是「放寬」還是「更緊縮」較難理解；第 39 頁 C 款、第 77 頁個資排除事由等，較近似直譯，好處是忠於原文，但可能影響全文的可讀性。	式在相當程度上適度地放寬了特種個資之應用」 「C.平等對待或平等機會：如果是為了在群體中辨識或者審查該群體間個別權利主體是否在機會或待遇上，就強化實現平等原則平等而有必要處理特種個資者，即應認為有公共利益存在。 此處所謂「群體間」所指為何？因為要處理的是特種個資的問題，所以指的是不同種族間之人、不同宗教或哲學信仰群體間之人、不同生理或心理健康狀態群體間之人、不同性取向群體間之人等。 須注意者，此處關於平等對待或平等機會相關之公共利益，解釋上不包括對特定個資當事人就平等對待或平等機會而給予之目的，也就是不包括可以在該等群體內特定之個人。例如，就身障者給予特殊照顧的情狀下，需審核該身障者群體間當事人之特種個資（健康資料），以確認是否符合所謂身障者之條件而予以對待，此係公共利益；但不得特別僅針對某特定人審查其健康資料辨識該特定人是否為身障者。再者，該等因審查而處理特種個資之行為不得造成實質損害或個人	25、52

編號	委員	建議	研究團隊回應	頁次
			之心神上痛苦 。」 「GDPR 第 89 條的科學與歷史為目的之研究特權，事實上還包含其他例外地允許處理個資事由：作為特種個資之例外允許處理情狀；於第三人獲得個資時，關於透明原則義務要求之減緩；個資留存期間限制之延展；以及作為豁免個資控管人責任之事由。」	
10		建議在結論章節，將討論編排順序重新調整，同一議題或同一標題下，分別就英國、德國論述，再以共通性的觀察或結論、統整歸納、並以對我國的建議作為小結。	感謝委員建議，此部分本報告於第肆部分「台灣、德國及英國個人資料保護法制之比較、分析」以及第伍部分重新調整編排。	
11		承上，結論部分是否能有共同或統一的見解，例如特種個資之利用，借鏡英國與德國落實 GDPR 的經驗，並非如同大家所想的有越來越嚴格的趨勢，報告在英國、德國部分分別有提到此一觀察，但結論部分沒有，僅表示德國法部分看來似有放寬的跡象；在去識別化方面，雖然有意見認為我國目前對去識別化的定義不清楚，但若從德國與英國的實踐來看，再進一步明確化「去識	新增段落： 「就比較德國與英國落實 GDPR 之法律制度與政策實踐而言，具體來看二者因為內國法制度不同的關係而有所差異，但事實上也有共同之處。 首先，在監管機關方面，兩國咸認該等機關須具有獨立性，且因為考量個資保護與政府資訊公開之間法益競合機會頻繁而須進行權衡，因此均將此二職權交由同一機關執掌。此外該等機關之數量無論是否單一，均須「專責」個資保護事務。	144-145

編號	委員	建議	研究團隊回應	頁次
		別」的定義確實是有難度的事情，因此我國未來修法是否要訂定去識別化的規定，可以參考這兩個國家及其他國家(例如日本)之作法，作成建議。	在特種個資之處理方面，與一般大眾對 GDPR 係「全世界最嚴格的個資法」觀念略有差異，事實上在兩國實際落實的經驗下可以發現雖然該「規則」具有相當高的拘束力，但事實上 GDPR 本身有許多使會員國調和其內國法制與豁免部分緊縮處理之例外可能，似有放寬之跡象與空間。 在去識別化方面，雖然有意見認為我國目前對去識別化的定義不清楚，但若從德國與英國的實踐來看，再進一步明確化「去識別」的定義確實是有難度的事情，因此我國未來修法是否要訂定去識別化的規定，或許可以參考這兩個國家及其他國家(例如日本)之作法。 至於特殊處理之情形、自動化處理與做成決策以及當事人權利之面向，也同樣地因為 GDPR 有使會員國依據內國法律架構與實際情況而調和之空間（例如，在例外允許個資處理之條件出現「依照會員國法律」之規範），因此可見到處理個資條件之鬆綁，並伴隨限縮當事人權利行使之結果，以及對於個資控管者為一定保護個資之措施要求。再者，此部分也都多有框架性規範，並配合特	

編號	委員	建議	研究團隊回應	頁次
			別法或指引作為補充。須注意者，無論是德國或是英國之規範對於此，仍有關於基本個資保障原則及對當事人權利保護之要件，而實務上兩國最常出現之關於自動化做成決策例外經當事人同意得處理個資例子也都為保險契約，但是仍有採行適當維護當事人權利措施之條件限制。」	
12		特殊處理情形方面，觀察臺灣現況，個別法律會規定「依個人資料保護法規定辦理」，指回適用個資法；換言之，當其他法規利用到個資且要訂定個資蒐集、處理、利用辦法時，各部會都會說按照個資法規定處理。與德國法或英國法比較，這是跟我國明顯不一樣的地方，結論可能會有兩個，其一：直接於個資法訂定框架規定；其二：個別領域因其特殊性，應針對各個不同的法規進行修正；由各機關負責訂定法規及執行，但這與單一監管機關的制度是否會有矛盾？在德國法部分較為特殊，較不會產生這類問題，假設我國未來成立個人資料保護委員會，勞動部訂定涉	新增說明段落於結論：「故針對特殊處理情形，若能於個資法中為框架性規定，對於規範之一致性及對個人資料保護之完整性，應當有所助益。不過，在現階段未有個資保護專責監管機關之情形下，不妨維持由各目的事業主管機關訂定相關指引，以儘速整合各領域相關個資保護之問題。另方面，在個資保護與其他特殊權利類型較可能發生競合之領域，如通訊傳播、生醫健康研究應用、勞動保障等領域，則因其特殊性，應由各機關負責針對各個不同的法規進行規範或修正並執行。在此則必須考量如該等規範係由個別領域之主管機關制訂與執行，則倘若未來如有個資專責監管機關時，該二個（或以上）機關間權限相互衝突時又應如何處理？	147-148

編號	委員	建議	研究團隊回應	頁次
		及勞工個資之相關法規，應以誰的意見為主？各主管機關與中央監管機關權限有衝突時該如何處理？建議研究團隊可以稍作補充。	本報告就此認為，如在個別領域就個資保護範圍競合時，應由個資保護主管機關就此部分表示意見，並且尊重其意見。首先，各部會就個資保護事務未必均能掌握，而個資專責監管機關所能涵括之權限範圍，就英國與德國看本來就遍及各領域。再者，以前述英國關於政府資訊公開及個資保護發生競合為例，在檢驗之流程上如果所涉及之個人資料主體即為該申請政府資訊公開案件之當事人，則應循 GDPR 或 DPA 2018 下的個資近用權請求，而非與之競合的政府資訊公開規範。」	
13	法制協調中心	依照 GDPR 規定，監管機關須具獨立性，且有人事、預算、裁罰等權限，爰本報告將 DPO 放在監管機關章節下似有未妥，且可能誤解未來我國設置 DPO 即符合歐盟監管機關之要求，爰建議將 DPO 移列至後面單獨章節討論。	英國法部分，新增第七節獨立處理 DPO。德國法部分，雖未單獨移列，但以附加說明方式處理。	73-79
14		本計畫需求書所列第 2 個研究議題為「個資特定目的外利用之要件」，英國法僅分析特種個資而未分析一般個資之目的外利用要件，建議於英國部分予以補充。	補充段落： 就個資特定目的外利用而言，英國 DPA 2018 並無特殊規範，原則上均參照 GDPR 之規範：在 DPA 2018 的第 87 條，規範即與 GDPR 如出一徹。	20-21

編號	委員	建議	研究團隊回應	頁次
			事實上 ICO 認為 GDPR 並沒有完全禁止目的外利用，而僅是需合於一定之限制條件。 從本質上講，如果個資處理的目的隨時間而改變，或者控管者想將資料用於其原本未曾想到的新目的，則控管者只能在以下情況下進行：1.新目的與原始目的兼容；2. 控管者出於新的目的獲得了個資當事人的特定同意； 3. 依據明確的法律規定，而該規定要求或允許出於公共利益的目的進行新的處理，例如公共機構的新功能等。而如果個資控管者對該原蒐集個資的新目的與用途是兼容(compatible)的，則無需新的合法依據即可進行進一步處理。但是，如果個資控管者最初是在同意作為蒐集個資的基礎，則通常需要再次獲得同意，以確保個資控管者的新處理合於公正、合法原則。 就 GDPR 與 DPA 2018 言，所謂「兼容」指的是出於公共利益的存檔目的、科學或歷史研究目的和統計目的之處理。並考量個資控管者的原始目的與新目的之間的任何關係、個資控管者最初蒐集個資當事人資料的環境，尤其是個資控管者與個資當事人的關係以	

編號	委員	建議	研究團隊回應	頁次
			及他們合理期望的結果、個人資料的性質，例如其是否特別敏感、新的處理行為可能對個資當事人產生之後果，和是否有適當的保護措施，例如加密或假名化等作為。 通常，如果新目的與原始目的非常不同，令人意外或對個人造成不合理之影響，則可能與個資控管者的原始目的不符。事實上，個資控管者通常可能需要徵得特定同意才能使用或揭露用於此類目的的資料。 綜言之，此部分英國並無異於 GDPR 之特殊規範。	
15		當事人權利的部分，德國法部分係將 GDPR 當事人查詢、告知、刪除等相關權利，就 GDPR 授權各國得為限縮規定部分逐一分析；惟英國法部分僅針對兒童權利進行分析，建議參照德國法將 GDPR 相關當事人權利於英國法予以限縮部分逐一分析。	新增段落： GDPR 第 23 條賦予會員國一定之調整空間,得以內國法限縮 GDPR 所規範當事人權利相關之適用要件。對此，英國 DPA 2018 於附件 2 第 3 部分與第 4 部分加以限縮權利之適用要件，而前者處理第三人權利，後者規範 GDPR 第 13 條及第 14 條之告知義務、第 15 條之查詢權，並鬆綁前述三個條文對應在 GDPR 第 5 條之相關原則(a)至(c)。 此間，第 19 條排除含有法律專業事務，使得法律專業在訴訟相關程序上，享有特權；第 20 條規範	64-66

編號	委員	建議	研究團隊回應	頁次
			關於自證己罪之當事人權利問題，亦即在法院審理中或在法院審理前藉由陳述等表明自己與某一犯罪有關或將使自己受到刑事指控的行為時，任何人無須遵守所列的 GDPR 規定，只要其遵守程度會通過揭示犯罪的證據而使該人面臨針對該罪行的訴訟程序即可。第 21 條規範關於公司財務，使得 GDPR 規定不適用於在滿足條件 A 或條件 B 的情況下為相關人員提供的公司財務服務或與之相關的已處理個人資料。條件 A 是相關 GDPR 規定的應用可能會影響某（金融）工具（即貨幣或對應替代之憑證）的價格。條件 B 為相關主體合理地認為，將 GDPR 所列條款應用於相關個人資料可能會影響以下個人的決定（第 21(3)條參照）： （i）是否買賣、認購或發行票據/憑證，或（ii）是否以可能對商業活動產生影響的方式行事（例如，對個人的產業戰略，企業的資本結構或企業或資產的合法或實益擁有權產生影響），和 GDPR 規定應用於該個人資料將對金融市場的有序運行或經濟體內資本的有效分配產生不利影響。 第 22 條規範管理預測，明訂	

編號	委員	建議	研究團隊回應	頁次
			GDPR 規定只要這些規定的應用可能會損害業務或活動的進行之虞，則不適用於基於與業務或其他活動有關的管理預測或管理計劃目的而處理的個人資料。第 23 條規範協商（契約法上之磋商過程）所列 GDPR 規定不適用於包含個資控管者與任何談判有關的意圖記錄的個人資料，但前提是該等規定的應用可能會損害這些談判方有適用。 第 24 條調和秘密參考來源，對此 GDPR 規定不適用於出於以下目的而秘密提供的（或將要提供的）參考資料所構成的個人資料：(a) 對個資當事人的教育，培訓或就業（或預期教育，培訓或就業）；(b) 個資當事人作為志願者的安置（或預期的安置）；(c) 個資當事人作為對任何機構官員任命（或預期的任命）；或 (d) 任何服務提供（或預期提供）。最後，第 25 條則針對考試題目與分數，做出個資當事人權利之豁免規定。	
16		德國、英國與我國個資法的比較，建議將本研究 6 項議題逐一列表分析較為清楚，或是如同劉老師的建議以議題式的編排做分析。	已依照劉委員建議修改。	

編號	委員	建議	研究團隊回應	頁次
17		第 50-51 頁，英國法關於去識別化資料於政府資訊公開、開放資料如何適用之部分，因報告僅簡單帶過，是否可以請研究團隊就這個部分補充說明。	新增段落： 進一步言，在很多情狀下該等資料僅僅適用於第三方再利用篩選過的資料的有限披露或公開，而不適用於大量的資訊公開（如政府資訊公開）以及許可條件下的政府資訊再利用（PSI）。關於此，本研究作者之一曾於其他論述歸納目前國際上對於政府所擁有資訊之接近及利用，可以化約為三個不同之模式，該三模式並可以其進程歸納為三個階段：政府資訊公開(Freedom of Information, FOIA)階段、公部門資訊再利用(Re-use of Public Sector Information, Re-use of PSI)階段、以及開放政府資料 (Open Government Data)階段。 在後二階段， 政府對於資料之再利用有以下三種選擇:(1)不公開個人資料作再利用；(2)將個人資料轉換成匿名形式(通常會轉換成聚合性的統計資料)，且僅公開已經匿名化處理的資料作再利用；(3)公開 個人資料作再利用。此時公務部門必須相對應有所作為，以便達成 PSI 再利用之目的。 關於新興科技發展的隱私與個人資料保護風險問題，因為科技於深度應用化後較難加以控制與改	31-33

編號	委員	建議	研究團隊回應	頁次
			變之關係，如果能在科技研發的早期即導入風險避免與風險識別之概念，則較為有效。不過科技於早期設計研發階段其未來影響較難以預估，因此造成早期介入風險防止之困難度與真正確切實效問題 。因此在確定何時以及如何發布匿名資料時，基於公開資料的原因將影響資料控管者進行揭露的方式，會因為身份識別的風險和後果會有所不同，一旦依據開放政府資料之許可而公開了資料，就可能無法保護其免於進一步利用或揭露或確保其安全。因此在資訊公開或政府開放資料時會因為範圍更廣而造成風險更大。 須注意者，儘管匿名資料屬於許可開放的範圍，而開放政府資料之許可即便是明確規定不允許使用者和再使用者以能夠進行重新識別的方式使用資料，但是，實際上這可能難以執行或甚至無法執行。 又，既然匿名及聚合的資料庫不應該允許對某個人再識別，因此在解釋上不應包含有任何的個人資料。為使得開放之資料有其真正之實用性，資料匿名化因個人資料的處理需不可逆轉的方式防	

編號	委員	建議	研究團隊回應	頁次
			止身份識別。進行相關操作時，資料控制人應先考慮一切用於識別身份的「合理可行」(likely reasonably）方法（不論是資料控制人還是任何第三方均為如此)，才考慮其他的相關因素或要件。	
18		第 94 頁最後一行「可進行單純自動化決策的三種例外情況簡單舉例」，後面未說明例外狀況為哪三種、第 174 頁最後一段提及巨量資料再利用可區分三種不同情狀，後面也未說明哪三種情狀，建議引註說明；第 212 頁德國個資法第 23 條，第一段應為該條的第 6 點。	1. 新增說明： 「另就可進行單純自動化決策的三種例外情況簡單舉例。這三個例外狀況包含： 1.個人或家庭活動：在純粹的個人或家庭活動過程中處理個人資料而與專業或商業活動無關者，因為不在 GDPR 的範圍內，故當然可進行單純自動化決策。2.執行法律：主管機關基於執法目的處理個人資料亦不在 GDPR 的範圍內（例如，警方調查犯罪)，相反地，此類處理應遵循 DPA 2018 第 3 部分中的規則。並且，Law Enforcement Directive 第 11(1)條則規範有經個資控管者受拘束之歐盟法或會員國法授權，且為該資料當事人之權利與自由提供適當安全保護措施者（至少有權對個資控管者部分為人為介入)，不在此限。3.國家安全－為維護國家安全或國防目的而處理的個人資料不在 GDPR 的範圍內。換言之，	63

編號	委員	建議	研究團隊回應	頁次
			雖然事實上 DPA 2018 關於 GDPR 之適用的第 3 章第 2 部分涵蓋了該內容，其中正包含對國家安全和國防的豁免。」 2. 新增註腳： 「此三種情狀為： ・情狀 1:該個資當事人(A)並不知悉其個人資料已被他人(B)，通常為個資控制人，但部分情狀下亦可能僅為個資儲存或利用人) 處理與利用; •情狀 2:B 違反 A 之自由意志而對於 A 之個資加以處理與利用;以及 ・情狀 3:A 表明放棄個資保護諸權利所保障之利益。 關於各情狀之討論，詳參：翁逸泓，2018 年 3 月，科技人權－全民電子通訊監察與個人資料保護，臺灣民主季刊，第 15 卷第 1 期，頁 23-24。」 3. 附錄一中就德國個資法第 23 條第 1 項之翻譯，補列第 6 款之標號。	137

歐盟國家個人資料保護法制因應GDPR施行之調適－以德國與英國為例

共同主持人：
李寧修　教授
翁逸泓 副教授

May 2020

國家發展委員會 法制協調中心

總說

2

- 國發會法協中心任務：
  - 行政院於 107 年 5 月 24 日院會責成國發會儘速成立「個人資料保護專案辦公室」，辦公室已於 107 年 7 月 4 日正式運作，二大工作重點之一厥為對於GDPR取得歐盟之**適足性認定**(adequacy decision)。
  - 我國相關機關為**促進產業發展**，節省個別產業法遵成本並避免法律風險起見，積極推動適足性認證。

研究架構

3

第一章 前言

第二章 英國個人資料保護法制介析及落實GDPR之實務狀況

- 第一節 法制沿革
- 第二節 英國個人資料保護之法制框架及其特色
- 第三節 英國個資法因應GDPR之法制調適與落實情形
  - 監管機關之中央與地方權限
  - 個人資料特定目的外利用之要件
  - 去識別化之要件、程序、認定方式等規定
  - 特殊處理情形
  - 自動化機器做成之決定
  - 當事人權利

研究架構

4

第三章 德國個人資料保護法制介析及落實GDPR之實務狀況

- 第一節 法制沿革
- 第二節 德國個人資料保護之法制框架與特色
- 第三節 德國個資法因應GDPR之法制調適、落實情形與脫歐前調適
  - 監管機關之中央與地方權限
  - 個人資料特定目的外利用之要件
  - 去識別化之要件、程序、認定方式等規定
  - 特殊處理情形
  - 自動化機器做成之決定
  - 當事人權利

第四章 臺灣、德國及英國個人資料保護法制之比較、分析

- 第一節 我國個人資料保護法制之現況與課題
- 第二節 臺灣、德國及英國個人資料保護法制之比較

第五章 結論與建議

英國監管機關

- 強化監督機制之必要性：沒有一個獨立專責監管機關，則幾乎完全無法具體面對數位時代下資料治理的根本問題，以及GDPR帶來的個資保護新制度挑戰
- 英國之ICO採取較為中央集權之制度，對於非公務機關例如中小型企業之需求採取所謂一站式服務，由ICO直接監理。與德國之聯邦制度不同。
- 分流處理：對中小企業、對DPO與對一般個資當事人
- 投入相當資源

英國監管機關

- 獨立個資專責機關
  - 分別地針對不同需求群體做出分層分流，目標導向的行動
  - 有效善用DPO作為ICO與民眾及私人組織的連結

英國監管機關

- 獨立個資專責機關
  - 分別地針對不同需求群體做出分層分流，目標導向的行動
  - 有效善用DPO作為ICO與民眾及私人組織的連結

英國去識別化

- 產業使用個人資料所遭遇的最常見難題：
  - 去識別化在我國個資法與相關法制架構中，意義混淆不明

英國去識別化

- 判斷一個自然人是否可識別，則其判斷標準應考慮資料控制人或任何其他人通常自行決定可能使用的所有手段
- 匿名化與假名化二者之區別標準在於判定何種結果才屬於可接受的資料再識別風險

英國特殊處理情形

- 個人資料保護與言論及資訊自由（GDPR第85條）
  - GDPR給予調和空間，但DPA 2018減縮個資保護調和
  - 實踐：BBC編輯指引(BBC Editorial Guidelines)、英國通訊管理署廣播指南(Ofcom Broadcasting Code)、編輯實踐準則(Editors' Code of Practice)
  - GDPR 85條保護的標的是關於任何學術領域之表意與資訊權利，而授權會員國以立法之方式調和其與個資保護之競合，與89條不同

英國特殊處理情形

- 官方文件之供公眾接近使用與處理（GDPR第86條)
  - 判斷在FOIA與EIRs之程序中是否有涉及在DPA 2018規範定義下之個資
  - 判斷是否為最常涉及之個資保護原則為合法、公平與透明原則
  - 衡量是否違背個資當事人之拒絕權
  - 判斷是否係個資當事人接近利用要求之例外情狀，並考量是否不揭露資料能維護公共利益
  - 要求相關機關負擔確認資訊與拒絕資訊公開之義務

英國特殊處理情形

- 官方文件之供公眾接近使用與處理（GDPR第86條)
  - 並不是一定被判定為個人資料或個人隱私事項，即不得公開，而是必須判斷保護的法益之間彼此的衡平

英國特殊處理情形

- 國家識別代碼之處理（GDPR第87條）
  - 無國家之統一識別代碼
  - 思考：是否必定要有身分證制度？

英國特殊處理情形

- 僱傭（勞動）關係資料處理（GDPR第88條）
  - 關於勞動與僱傭方面之個資保護規範可能散落各法
  - 英國DPA事實上對勞動或僱傭範疇的個資特別豁免或管制事項並未有太多的直接規範
  - 僱傭實務準則(the employment practices code)
    - 應徵與選才(Recruitment and selection)
    - 僱傭紀錄(Employment records)
    - 工作監管(Monitoring at work)
    - 勞動者健康狀況(Information about workers' health)

英國特殊處理情形

- 僱傭（勞動）關係資料處理（GDPR第88條）
  - 在被預先告知的情況下，則似乎可以因為無合理隱私期待而受一定程度監控或介入
  - 毫無保留的要求應徵者個資，也為DPA所不許
  - 透明原則

英國特殊處理情形

- 基於公益之檔案儲存目的、基於學術或歷史研究目的以及統計目的之處理（GDPR第89條）
  - 以科學研究或歷史研究為目的之個資處理，應受適當技術上及組織上保護措施之拘束，該等保護措施得包括假名化，**但須於實現以科學研究或歷史研究為目的之範圍**，且不允許或無法再識別個資當事人
  - 調和之態樣有許多不同型態

英國特殊處理情形

- 特殊處理情形：與其他基本權利保障事項之調和
  - 個資保護與言論及資訊自由：台灣似無相關指引或政策方向
  - 並非被判定為個人資料或個人隱私事項即不得公開，而是必須判斷保護的法益之間彼此的衡平
  - 是否仍需要身分識別制度？
  - 採取針對不同需求者，分別給予不同的勞資權利保障宣導

英國自動化決策

- 台灣個資法對個資當事人之權利保障並未跟上數位/AI時代發展需求：機器自動化做成決策的法規真空
  - 科技部人工智慧科研發展指引
- 歐盟：「可信賴的人工智慧道德指引(Ethics Guidelines for Trusted AI)」，其中三個貫穿整個指引的基本要素乃係：首需合法，其次要合乎道德，最後必須要「穩健(robust)」

英國自動化決策

- 英國：資料自動化決策與資料剖析細部指引
- 企業、組織為因應GDPR而需特別留意或做出改變的事項
  - 記錄資料處理活動
  - DPIA
  - 提供給資料當事人的隱私權資訊
  - 申訴、異議與獨立審查程序與機制

當事人權利：兒童權利行使

- 此處範圍僅限縮在資訊社會服務，但我國卻無對應規範
- 資訊社會服務(Information Social Service, ISS)
  - 關於技術規則與資訊社會服務領域相關資訊之程序指令
  - 通常以一定距離，通過電子方式並應服務接受者的個人要求提供有償服務的任何服務
    - 提供服務時各方沒有同時出席
    - 向最終使用者免費提供但通過廣告資助的線上遊戲應用程序或搜索引擎，仍屬於ISS的定義範疇內

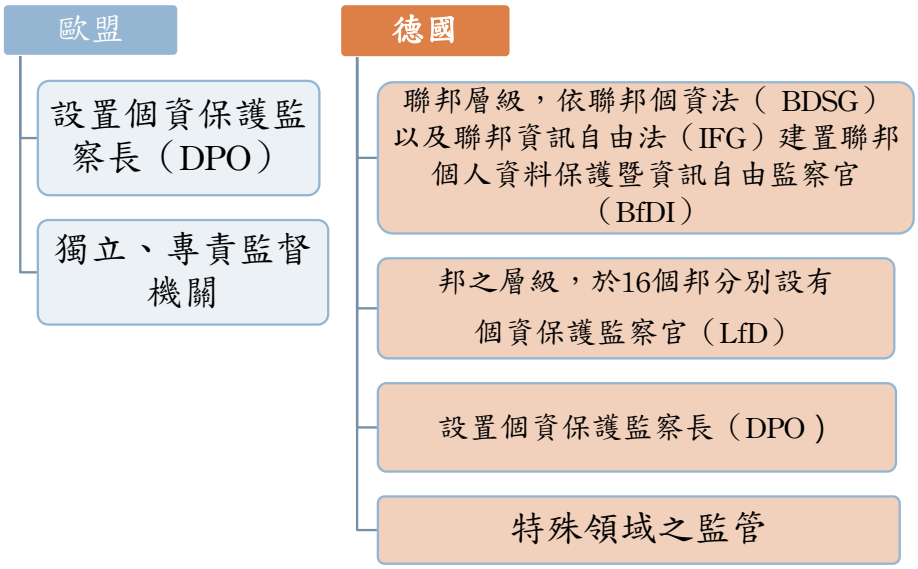
當事人權利：兒童權利行使

- 資訊社會服務(Information Social Service, ISS)
  - 適合年齡設計準則
  - 應用符合比例且以風險為基礎(proportionate and risk-based)之考量方法

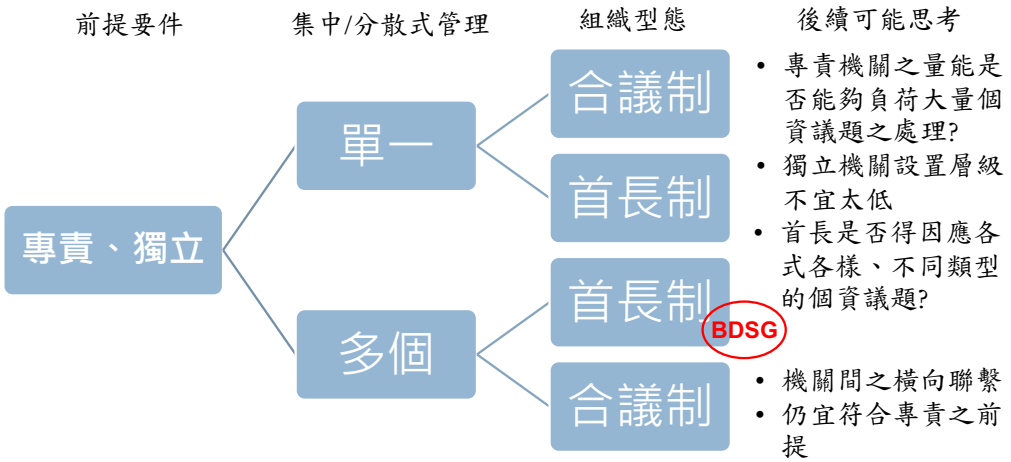
其他

- 公務機關、非公務機關與公共利益的難解糾葛
  - 個資法無利益衡量之條款
  - 「公共利益」這個不確定法律概念加乘「必要」的比例原則操作衡平概念的困難
- 通訊傳播、生醫健康研究等個別產業面向間與個資保護之交錯問題，或許應有專門規範

德國監督機關



德國監督機關



德國特種個資目的外利用之要件

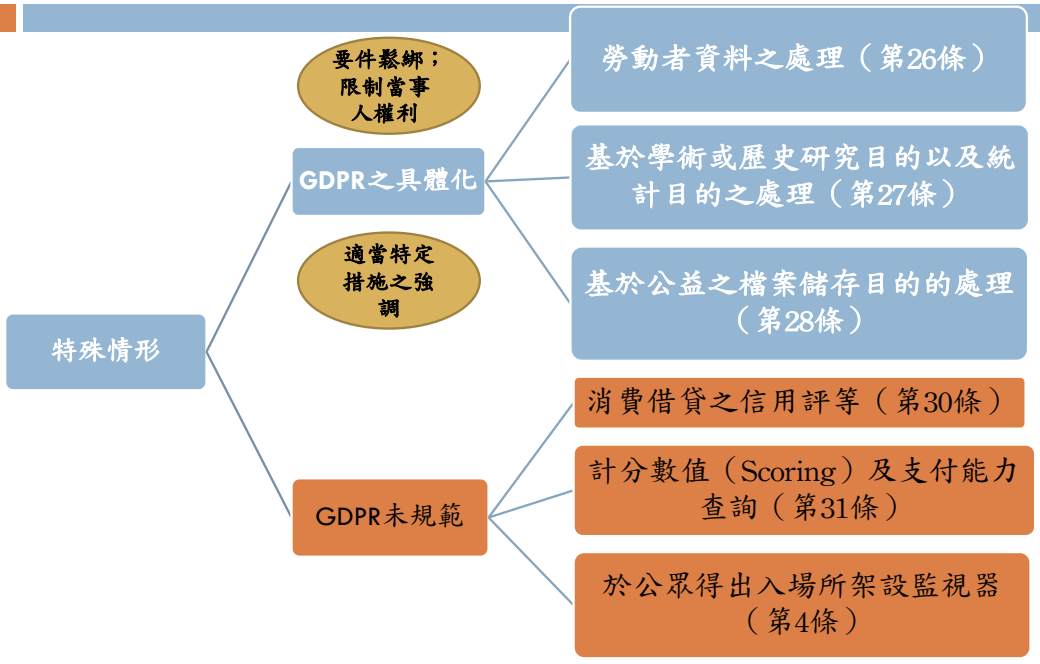
德國特種個資目的外利用之要件

- 德國個資法第23條第2項（公務單位）及第24條第2項（非公務單位）
- 具備**一般個資目的外利用**之要件
  - 公務單位：德國個資法第23條第1項
  - 非公務單位：德國個資法第24條第1項
- 應符合**處理特種個資之要件與程序**
  - GDPR第9條第2項，或
  - 德國個資法第22條
    - 公務及非公務單位（德國個資法第22條第1項第1款）
      - 基於社會權之行使或因此而生之義務
      - 基於健康照護、醫療、社福照顧或處置
      - 公共健康領域之公益維護
      - 基於重大法益且有急迫、必要
    - 公務單位（德國個資法第22條第1項第2款）
      - 重大公益之維護＋必要性＋法益權衡

適當且特定措施之採行

- 以德國個資法第22條第2項所定適當特定措施為主，並作為合法處理之要件之一，可能之措施有：
  - 依據GDPR所應採行之技術及組織上措施
  - 事後追溯個資使用歷程之措施
  - 處理過程中相關人員個資保護意識之提升
  - 任命個資保護監察長
  - 處理個資地點之管制
  - 假名化
  - 加密
  - 處理系統運作與應變
  - 進行經常性查核、評估
  - 就目的外傳輸建立特殊程序規範
- 於特殊處理情況中再強化特定措施，例如:
  - 匿名化
  - 刪除義務

德國特殊處理情形

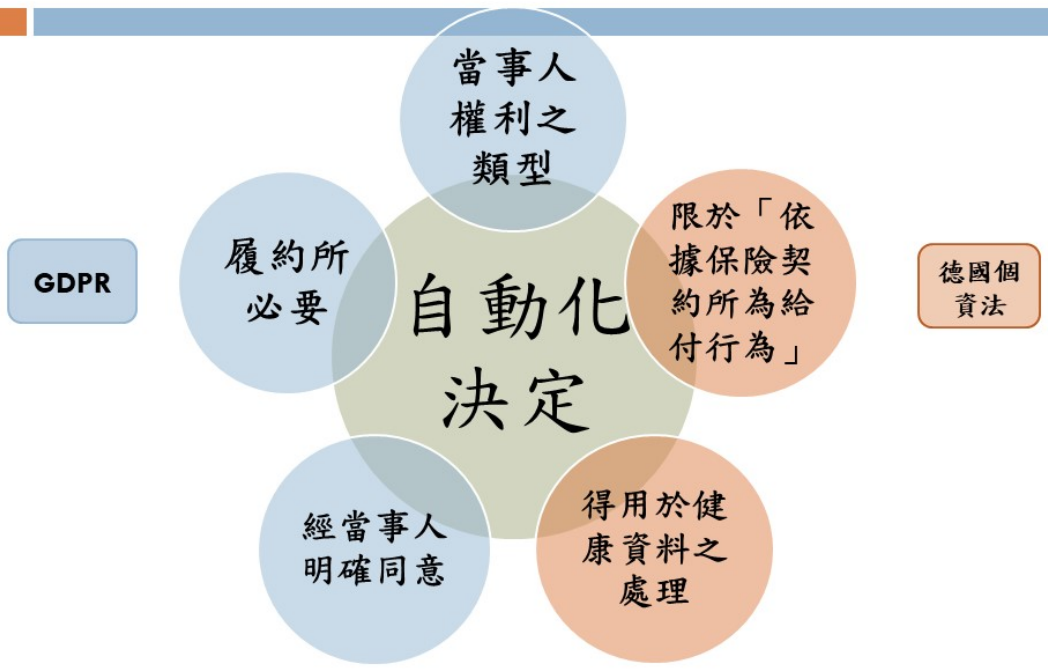


德國特殊處理情形

29

- 德國個資法對於特殊處理情況，原則上係對GDPR所定處理要件為鬆綁，並大多因此伴隨著限縮當事人權利行使之效果。
- 但亦要求控管者
  - 採行適當特定措施，例如:
    - 強化告知義務
    - 當事人同意有效性之確認
- 屬框架性規範，仍允許可透過特別法就細節為補充。

自動化決定



當事人權利

針對GDPR所定以下當事人權利，擴大排除適用之範圍：

- 免除告知義務
- 限制查詢權
  - 基於科學或歷史研究目的以及統計目的之資料處理
  - 基於公共利益之檔案儲存目的之資料處理及德國個資法第29條針對負有保密義務情況
  - 限縮GDPR第17條第1項所定刪除之權利
- 限縮異議權之主張範圍
- 輔以法益權衡條款，要求於個案中就當事人權利與處理個人資料之利益間為實質判斷，以求衡平

當事人權利

32

- 當事人權利
  - 就兒童權利保障未有明文，回歸適用GDPR之規定。但強調應對於孩童對提供個資行為所代表之法律上意義及效果，包括蒐集之目的、後續利用之範圍及其作為當事人所得主張之權利...等，是否具有充分的理解與認知能力，而不當然受限於特定年齡。

結論與建議

- 我國在法制上如要完善個資保護法制，甚至企圖實現良好的資訊治理，實有必要將法制更加以完備
- 一個獨立專責且能量充足的監管機關，是推動個資保護法制的必要機構性架構
- 針對去識別化之規範，建議可參考德國個資法採取集中規範的方式，以我國個資法施行細則第12條第2項為本，進一步參考GDPR或他國對於安全維護措施之普遍要求，予以強化

結論與建議

- 對於當事人權利之類型及其限制應以法律明確規範限制之要件輔以法益權衡條款以及相關配套
- 缺乏利益衡量之條款，也使得僵化而機械的文義解釋操作，令社會大眾尤其是產業界產生對於個資法制之恐懼
- 面對我國數位經濟發展政策的渴望，在個資保護法制上對包括人工智慧（機器自動化）決策、通訊傳播與健康研究應用等不同領域上，可以考慮「超前部署」，以其作為我國資訊治理政策的起點

謝謝聆聽