GDPR與個資法之動態檢討新趨勢

施弘文 專案經理
科技法律研究所 價值拓展中心
財團法人資訊工業策進會

stli 科技法律研究所 SCIENCE & TECHNOLOGY LAW INSTITUTE

hwshih@iii.org.tw
www.iii.org.tw

大綱

壹、前言

貳、監管機關及企業遵循GDPR之困境

參、GDPR與我國個資法動態調整之思索

肆、結語

大綱

壹、前言

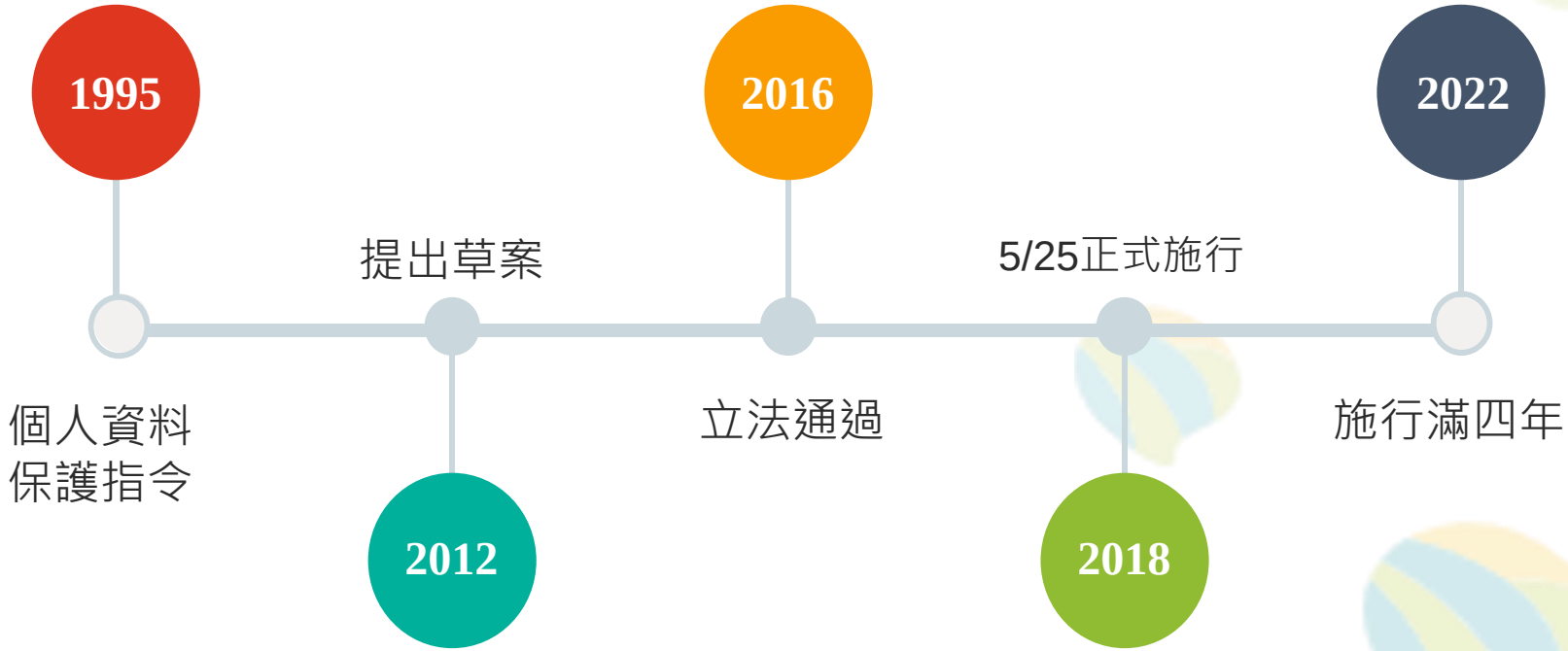
貳、監管機關及企業遵循GDPR之困境

參、GDPR與我國個資法動態調整之思索

肆、結語

壹、前言

※歐盟一般資料保護規則 (General Data Protection Regulation, GDPR)



壹、前言

透過發布指引持續細緻化

- 歐洲資料保護委員會(EDPB)陸續發布相關指引文件與建議，使規範內容更加明確與細緻，並讓規範標準有所依循。
- 至2022年9月，總共發布60個指引、6項建議，平均每年發布15個指引。
- 指引與建議的內容如說明各資當事人的權利內涵、資料控管者相關義務的細緻建議、行政罰款之計算標準、符合歐盟個資保護水準的傳輸建議、成員國監管機關於監管時的處理準則等。

資料來源：https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en

適足性認定協商

- 依GDOR第45條，歐盟區域人民個人資料的跨境傳輸，只有在特定第三國對個資保護的水準符合歐盟的認定時，方可進行。
  - 目前獲得歐盟執委會承認者包含英國、瑞士、日本、韓國、以色列等14個國家、地區。
  - 歐盟與美國於今年3月重新達成初步的跨大西洋資料保護框架（Trans-Atlantic Data Privacy Framework）。
  - 未通過「適足性認定」國家(如我國)之企業，若在歐盟設立據點，需特別留意資料從歐盟傳輸到境外時須遵循標準契約條款（Standard Contractual Clauses，SCC）。

資料來源： https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

資料保護官之設置

- 應設置資料保護官(DPO)之情形通常是：個資控管者或處理者之核心活動內容涉及大量經常性及系統性的個資監管，或大量特種個資(如種族、政治意見、宗教哲學信仰、工會會員身分、性傾向、性生活或刑事紀錄)時。
- DPO須具備個資保護相關專業知識及經驗，並獨立執行職務。而企業需給予DPO相關資源、權限，使其能向組織提供意見，若企業不採納DPO的意見，則以留存書面紀錄為佳。

資料來源： https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

壹、前言

GDPR與我國個資法之現況與影響

➢ GDPR成為各國個資法規範本

近年世界各國個人資料保護法規的制定或修正，或多或少都有參考GDPR，例如日本、韓國、中國、泰國、新加坡、加拿大、巴西。在美國，包含加州、維吉尼亞、科羅拉多、夏威夷、麻州、猶他、紐澤西等22個州在內之消費者隱私法案也都受到GDPR之影響。

➢ GDPR以鉅額裁罰威嚇大型企業

截至2022年9月，歐盟各成員國監管機關開出的裁罰金額總共超過20億歐元，包含Amazon、Meta、Google、WhatsApp等大型企業都陸續被裁罰數千萬甚至數億歐元。而為了法令遵循，如Microsoft、J.P.Morgan、IBM等企業設立個資保護單位加以因應。

➢ 我國個資法將啟動修正

因「健保資料庫」提供學術研究之爭議，我國個資法在今(111)年8月遭大法官宣告部分違憲，產生限期修法的探討。

大綱

壹、前言

貳、監管機關及企業遵循GDPR之困境

參、GDPR與我國個資法動態調整之思索

肆、結語

貳、監管機關及企業遵循GDPR之困境

主要問題	產業影響	說明
「一站式機制」造成裁決效率低落	一. 一站式機制之內涵與成果	說明一站式機制的法規內容，並舉例可能的適用時機，接著討論「領導監管機關」內涵，最後則說明當前機制下施行的成果。
	二. 效率低落之緣由與案例	以歐盟各成員國所監管的企業數量，以及一站式機制的程序盲點，說明效率低落的可能原因，並佐以公益團體的投訴實例。
無法有效遏止跨國企業濫用個資，監管機關另謀他法	三. 網路平台業者擁有龐大個資且難受約束	平台業者所遭遇的處境，以及當前模式面臨的利益衝突。而不同法規間的差異，也大幅增加業者的合規成本。
	四. 成員國所採取之規避手段	成員國採用GDPR以外之法令，例如成員國之內國法以「繞過」GDPR。

貳、監管機關及企業遵循GDPR之困境

一.「一站式機制」之內涵與成果

緣由與內涵

歐盟為實現「資料單一市場」，於GDPR前言第127點說明，若爭議事件之資料管控或處理地涵蓋歐盟複數成員國，得提交至其中領導監管機關(lead supervisory authority)為爭端解決，並於本文§60以下創設「一站式機制」，使跨國業者只需面對1個而非27個監管單位。

適用時機

1. 企業進行跨境資料傳輸，且在歐盟有多數機構時。
2. 企業在歐盟僅一個機構，但處理歐盟複數成員國人民之個資時。

領導監管機關

✱GDPR§56(1)：資料控管者或處理者之主要分支機構…之監管機關，應有權做為…跨境處理時之領導監管機關。
✱GDPR§60(7)：領導監督機關應依其情形通過該裁決並告知控管者或處理者之主要分支機構...，並向其他相關監管機關及委員會通知該裁決…。

爭端解決機制

1. 領導監管機關先對事件提出裁決草案。
2. 其他監管機關得對裁決草案提出反對意見。
3. 若領導監管機關採納反對意見，需修正裁決草案後再向其他監管機關提交。
4. 若領導監管機關拒絕採納反對意見，則依GDPR§65(1a)送交EDPB發布「具拘束力之決定」，領導監管機關需以該決定為基礎做出裁決。

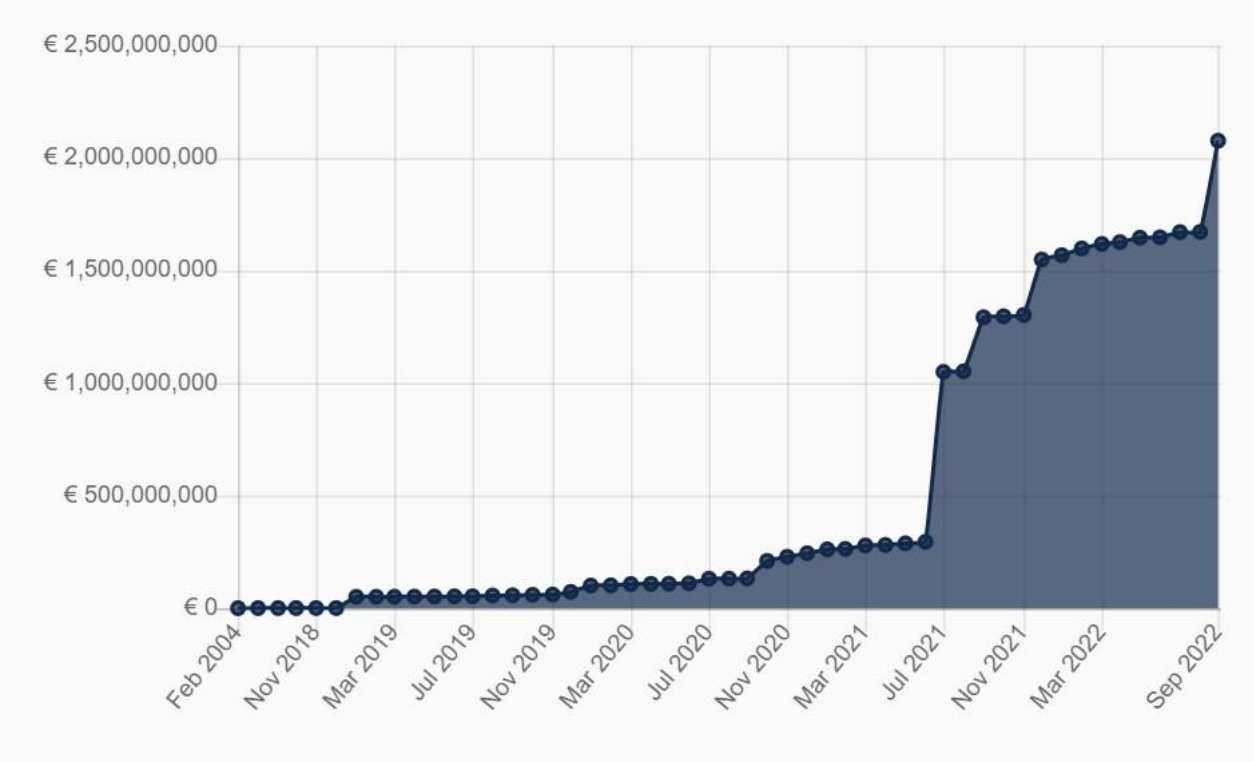
貳、監管機關及企業遵循GDPR之困境

一.「一站式機制」之內涵與成果

裁罰金額

裁罰金額累計：20億7671萬歐元

罰款總計前三名之國家依序為：
盧森堡(7.46億)、愛爾蘭(6.48億)、法國(2.71億)



資料來源：https://www.enforcementtracker.com/?insights

控管者	國家	罰款	日期
Amazon	盧森堡	7.46億	2021.07
Instagram	愛爾蘭	4.05億	2022.09
WhatsApp	愛爾蘭	2.25億	2021.09
Google	法國	9千萬	2022.01
Facebook	法國	6千萬	2022.01
Google	法國	6千萬	2021.12
Google	法國	5千萬	2019.01
H&M	德國	3千5百萬	2020.10
TIM	義大利	2千7百萬	2020.01
Enel Energia	義大利	2千6百萬	2022.01

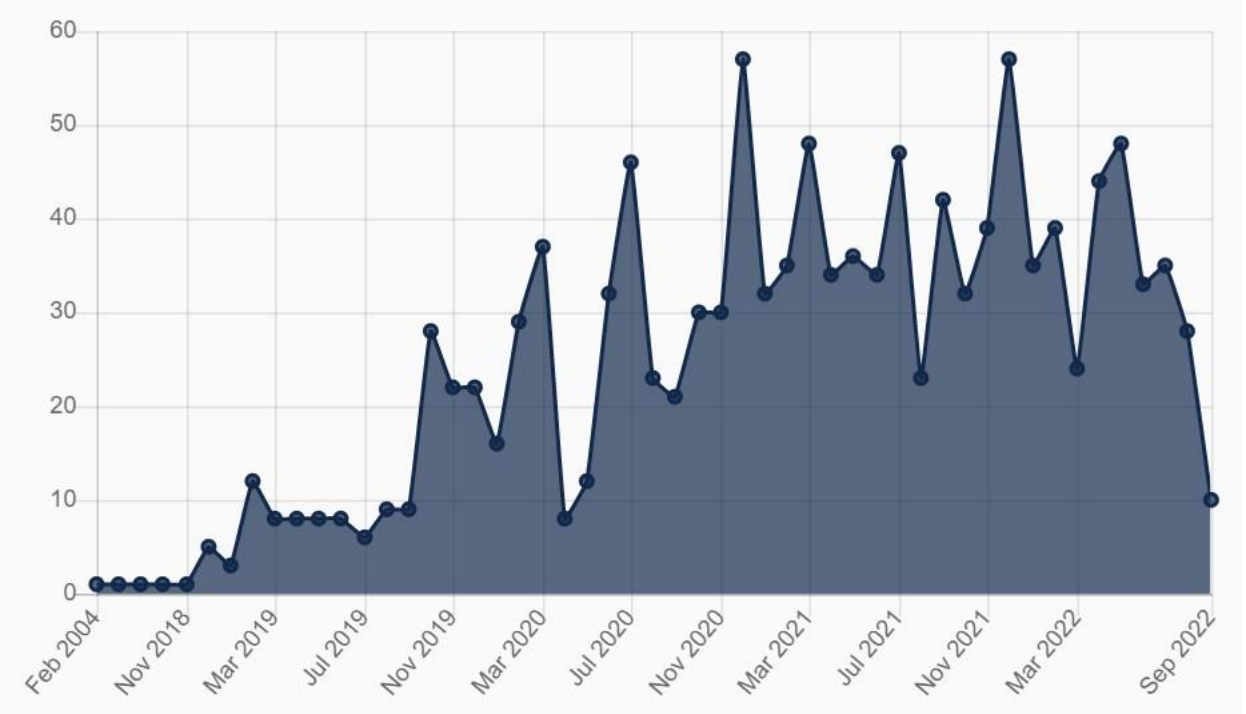
貳、監管機關及企業遵循GDPR之困境

一.「一站式機制」之內涵與成果

裁罰數量

裁罰數量累計：1249

罰款次數總計前三名之國家依序為：
西班牙(482次)、義大利(175次)、德國(112次)

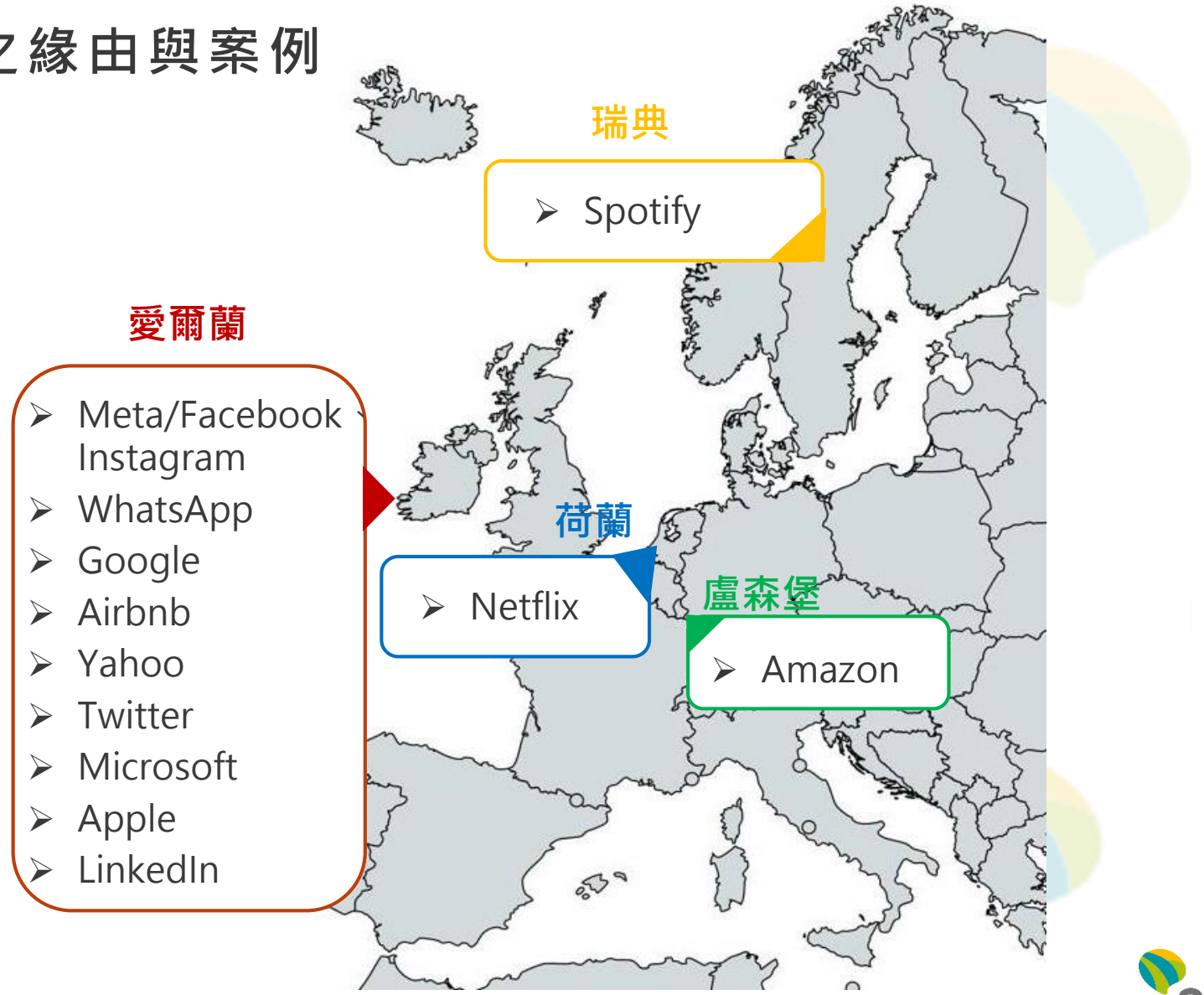


資料來源：https://www.enforcementtracker.com/?insights

國家	次數	罰款總額
西班牙	482	5千6百萬
義大利	175	1.38億
德國	112	5千4百萬
羅馬尼亞	97	80萬
匈牙利	49	140萬
挪威	48	929萬
希臘	44	3千萬
波蘭	39	339萬
比利時	37	179萬
法國	29	2.71億
盧森堡	27	7.46億
愛爾蘭	16	6.48億

貳、監管機關及企業遵循GDPR之困境

二.效率低落之緣由與案例

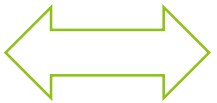


貳、監管機關及企業遵循GDPR之困境

二.效率低落之緣由與案例

爭端解決機制

1. 領導監管機關先對事件提出裁決草案。
2. 其他監管機關得對裁決草案提出反對意見。
3. 若領導監管機關採納反對意見，需修正裁決草案後再向其他監管機關提交。
4. 若領導監管機關拒絕採納反對意見，則依GDPR§65(1a)送交EDPB發布「具拘束力之決定」，領導監管機關需以該決定為基礎做出裁決。



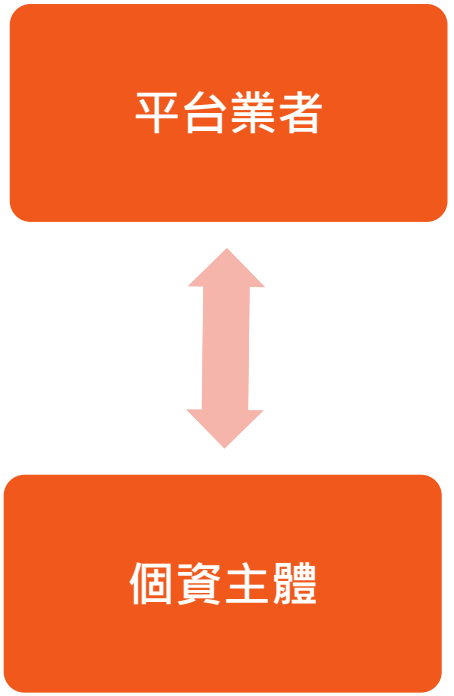
效率低落緣由

1. 違規事證一部分由各監管機關提供。
2. 各成員國監管機關每周都需要向其他監管機關發送數份草案。
3. 不同監管機關間反對之意見互相衝突，常常造成部分採納、部分反對之情形。
4. 完成一份裁決通常要在各監管機關間往返多次(最常提出反對意見者為德國)，且領導監管機關大多傾向不送交EDPB，以避免更難掌握裁決方向。

貳、監管機關及企業遵循GDPR之困境

三.網路平台業者擁有龐大個資且難受約束

平台業者及個資主體間關係



- 常概括、廣泛的條列蒐集目的及範圍。
- 具經濟優勢地位，主導同意條款之撰寫。

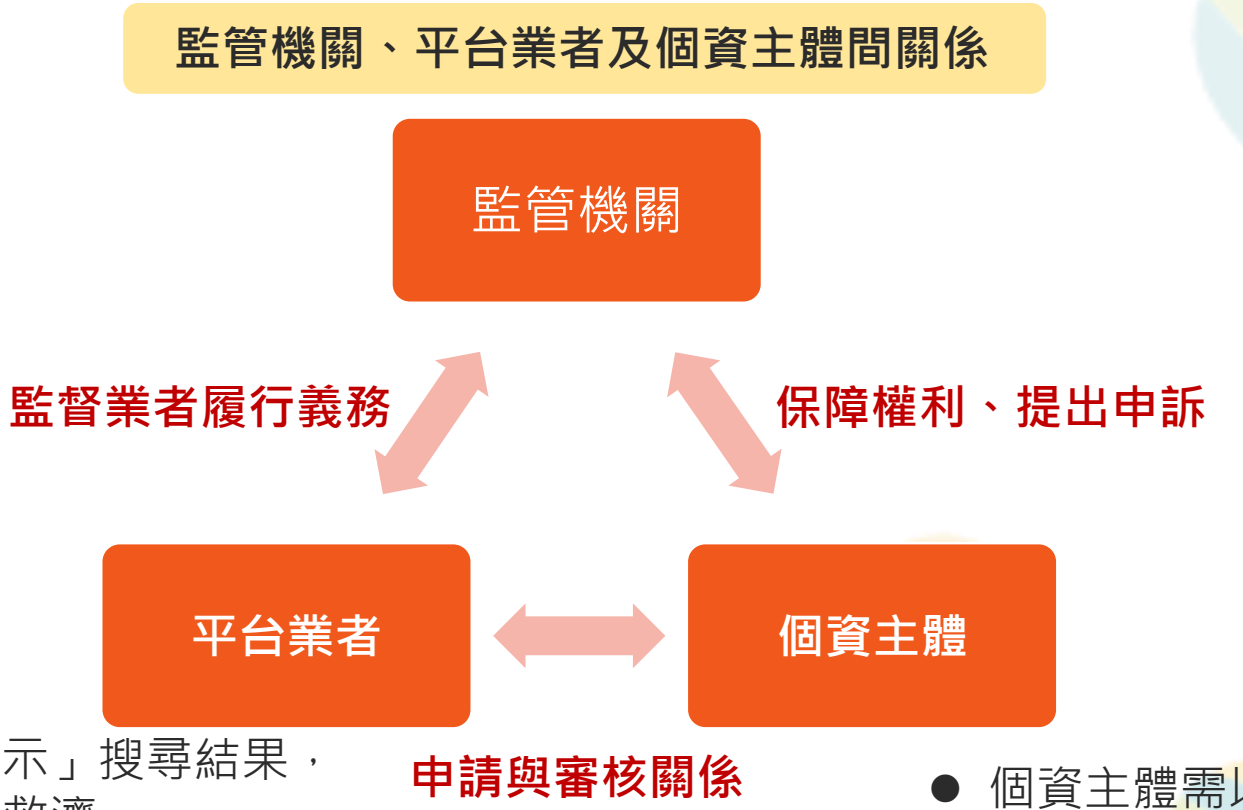
- GDPR§6「處理之合法性」
- 個資蒐集目的須特定、明確及合法，且不得為該等目的以外之後續處理(除外規定：§89)

- 難以逐一審查條列之項目。
- 難以掌握個資流向。
- 是否同意之空間受到壓縮。

貳、監管機關及企業遵循GDPR之困境

三.網路平台業者擁有龐大個資且難受約束

- 以GDPR§17「被遺忘權」為例
- 個資主體有權向平台(Google)要求移除關於自己的負面訊息或過時的個資、搜尋結果



- 業者若允許「不顯示」搜尋結果，受影響的網頁難以救濟。
- 業者審查將耗費大量人力，且標的難以特定。
- 「被遺忘權」使業者得審核網頁內容，形成私人言論審查。

- 個資主體需以欲遺忘之網頁頁面為標的，向搜尋引擎業者提出申請。
- 個資主體與該網頁的作者存在對立關係。

貳、監管機關及企業遵循GDPR之困境

四.成員國所採取之規避手段

(一)、裁罰背景與爭點說明(1/2)

- 近年Google、Facebook 屢因個資保護問題，遭法國個資主管機關國家資訊自由委員會(CNIL)裁罰。

2017/05
將使用者cookie用在**第三方網站便於投放個人化廣告**，造成使用者在「不知情的情況下」被追蹤，而裁罰15萬歐元

2021/12/31
「拒絕」cookie蒐集未與「同意」相同容易，且使用者介面設計不夠清楚，罰款6000萬歐元

2016/03
僅**將「被遺忘權」適用在歐盟境內**而非全球網域，罰款10萬歐元

2019/01
未向使用者**提供足夠資料同意政策，也未給予使用者對訊息足夠控制權**，裁罰5000萬歐元

2020/12
對使用者之cookie違法使用，違反《資訊技術、資料文檔與自由法》(下稱法國《個資法》)，罰款1億歐元

2021/12/31
網站中的使用者介面只有接受蒐集cookie的按鈕，並無提供類似的方式讓使用者拒絕蒐集，罰款1.5億歐元

貳、監管機關及企業遵循GDPR之困境

四.成員國所採取之規避手段

(一)、裁罰背景與爭點說明(2/2)

- 2020年6月，CNIL 依法國《個資法》任命報告員*調查兩家公司違法情形，調查在隔年9月結束並將報告告知兩家公司，使兩家公司得進行答辯， 並由CNIL組成「受限制委員會(Formation restreinte)」*進行審查。

	Google 案	Facebook 案
裁罰事由	用戶終端對cookie蒐集之拒絕或撤回「不同意」需與「同意」一樣容易	• 「用戶終端對cookie蒐集之拒絕或撤回「不同意」需與「同意」一樣容易 • 且使用者介面設計不夠清楚
裁罰依據(法律)	主要依據GDPR、法國《個資法》第82條	
裁罰金額	1.5億歐元 (GOOGLE LLC 9000萬元，GIL 6000萬元)	6000萬歐元
限期改善	限期3個月內改善，逾期每日處10萬怠金	
裁罰考量因素	• Google在搜尋引擎市場具壟斷地位並利用cookie獲利 • CNIL已盡通知改善義務	• Facebook在社交平台具領導地位，卻將第三方應用程式嵌入cookie應用在廣告獲利 • 更新仍未達改善標準

*註：
1.報告員:若違反法國《個資法》或GDPR時，受限制委員會可任命成員之一為報告原先做成調查報告。報告員可向受限制委員會提出報告，但不參與審議。
2.受限制委員會:由5名CNIL之委員組成，其中一人為主席，主席須為CNIL主席以外之委員，可對違反法國《個資法》或GDPR者進行裁處。

貳、監管機關及企業遵循GDPR之困境

四.成員國所採取之規避手段

(二)、歐盟已有統一的爭端解決機制，法國CNIL是否有裁罰權限？還是應適用一站式機制？

報告員：

歐盟電子通訊隱私指令(e-Privacy Directive)對cookie的規範，**已經依法國《個資法》第82條轉換為內國法**，CNIL可對不遵守該法之資料控制者或其代理人進行制裁

Google：

Google 歐盟總部於愛爾蘭，且歐盟個資保護主管機關已收到大量投訴Google 蒐集 cookie 之事件，故**有權裁處者應屬「愛爾蘭個資保護委員會(DPC)」**

受限制委員會：

本次程序僅涉及法國使用者之操作方式，而GDPR 已規定成員國可以自行決定監管單位，且此單位也可以是資保護機構以外的單位。**受限制委員會屬「電信監管機構」非屬個資保護單位，不適用「一站式機制」**(也就是主張本事件CNIL亦有裁罰權力)

大綱

壹、前言

貳、監管機關及企業遵循GDPR之困境

參、GDPR與我國個資法動態調整之思索

肆、結語

參、GDPR與我國個資法動態調整之思索

111年憲判字第13號【健保資料庫案】(111年08月12日)	
一. 現行規定	個資法第6條第1項第4款，有關病歷、醫療、...之個人資料，不得蒐集、處理或利用，但公務機關或學術研究機構基於...統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人，則不在此限。
二. 民間團體主張	未設行為法以節制國家權力行使，違反法律保留原則；當事人的退出權遭過度限制，也違反比例原則，因此聲請釋憲。
三. 憲法法庭判決	◆ 個資法第6條第1項第4款與法律明確性原則、比例原則尚屬無違，不牴觸憲法第22條保障人民資訊隱私權。 ◆ 現行法令欠缺個資保護之獨立監督機制，對個資隱私權之保障不足，而有違憲之虞。 ◆ 健保資料庫對外提供之目的、範圍、監督防護機制等事項，欠缺法律明確規定，應修正或制定專法。 ◆ 衛福部...就個人健保資料之提供公務機關或學術研究機構於原始蒐集目的外利用，...，欠缺當事人得請求停止利用之相關規定，違反憲法第22條保障人民資訊隱私權之意旨。

資料來源：https://cons.judicial.gov.tw/docdata.aspx?fid=38&id=309956

參、GDPR與我國個資法動態調整之思索

111年憲判字第13號【健保資料庫案】(111年08月12日)		
四.	內容引用GDPR	大法官於判決最後之註釋中，明確提及： 例如歐盟一般資料保護規則（General Data Protection Regulation，下稱GDPR）即規定各會員國應設置至少一獨立監管機關（supervisory authority），職司個人資訊隱私權之保障；該監管機關應依照GDPR規定獨立行使職權（GDPR第51條及第52條參照）。

資料來源：https://cons.judicial.gov.tw/docdata.aspx?fid=38&id=309956

參、GDPR與我國個資法動態調整之思索

個資法違憲判決之思索	
違憲爭點	產業之因應
一. 欠缺個資保護之獨立監督機制，對個資隱私權之保障不足，而有違憲之虞	➢ 目前我國個資法採「分散式管理」，依據產業類別而有對應之「中央目的事業主管機關」。 ➢ 惟我國刻正與歐盟洽談「適足性認定」且已受違憲宣告，未來修法若採GDPR之「獨立監管機關」亦屬可能的方向。
二. 衛福部...就個人健保資料之提供公務機關或學術研究機構於原始蒐集目的外利用，...，欠缺當事人得請求停止利用之相關規定，違反憲法第22條保障人民資訊隱私權之意旨	➢ GDPR係以「同意」或「法令」作為得利用個資之基礎，為採「選擇加入」之方式。 ➢ 然憲法判決要求法令應提供人民「選擇退出」之權利，就此部分與GDPR之規範不同。 ➢ 產業在合規性方向上可參考同樣有退出權(opt out)的美國加州消費者隱私法。

大綱

壹、前言

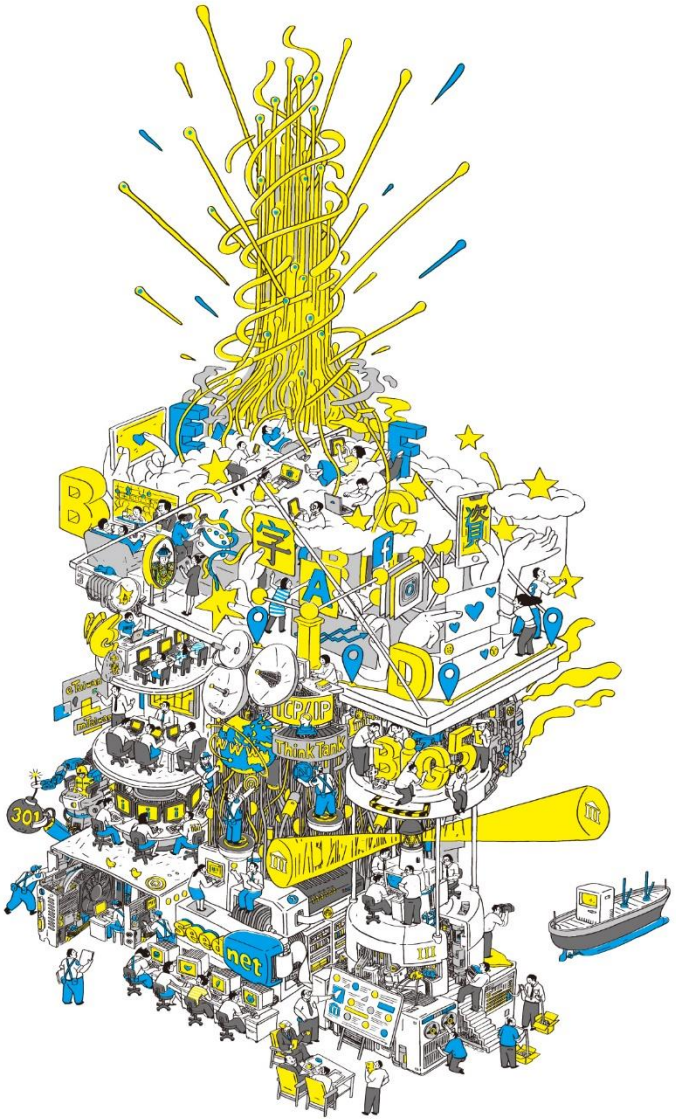
貳、監管機關及企業遵循GDPR之困境

參、GDPR與我國個資法動態調整之思索

肆、結語

肆、結語

- 目前僅有相關討論聲浪，即便修正變動幅度應不至於太大
- GDPR仍為隱私法規之領先規範，產業應留意不同區域間隱私法規之適用問題
- 在變動的時代中，更應留意法規之趨勢，與時俱進



1擘劃我國資訊工業發展藍圖 2開啟電腦中文化時代 3打造台灣資訊品牌 4培養台灣資訊人才
5開創產業顧問服務 6提升網路基礎建設 7E化政府系統 8普及網路應用人口
9建構資訊法案制度 10縮減城鄉數位落差 11推動數位內容 12推動數位科技外交
13策進 e-Taiwan / m-Taiwan 14精進5G智慧科技創新應用 15支援文創與設計產業奠基
16培育創新創業新動能 17擔任數位國家智庫 18活化原鄉無線寬頻環境
19協助產業拓展商機並強化資安防護 20數位轉型化育者

THANK YOU