

知情同意的介面設計： 因應暗黑模式下的歐盟管制趨勢

楊采文*

壹、前言

使用者可能發現在下載應用程式並安裝啟用時，頁面會跳出個資告知事項內容或是隱私權聲明連結，要點選「同意」才能進行下一步；或是在瀏覽網站時會跳出cookies政策，要求使用者「同意接受所有cookies」才能關閉視窗並繼續瀏覽網站。這些徵詢使用者同意的介面，在數位網路環境中相當廣泛而普遍，甚至成為我們日常生活中習以為常的環節。

由於當前資訊保護法制的核心，是確保資料蒐集活動的透明性，經由個資控管者在蒐集當下向個資當事人的告知或揭露，取得個資當事人的同意，作為個資控管者資料處理的依據。個資當事人經個資控管者在資料蒐集時進行告知，可知悉其個資流向、利用方式及後續請求刪除等作業之資訊，有助於個資當事人強化對於其資料的控制，此即為「知情同意」(informed consent)的運作邏輯。

依據各國個資法規差異，個資控管者除取得當事人同意以外，亦可仰賴法律明文規定

或履行契約義務等其他合法基礎作為蒐集依據，但考量到其他合法基礎有特定適用情境，當事人同意仍是個資控管者從事個資處理的主要合法基礎，因此，個資控管者在網路環境中，需要設計一個向當事人進行告知、取得當事人同意表示並記錄當事人同意結果的流程與介面。在取得個資當事人知情同意流程下，此介面如何設計，以兼顧法規遵循、使用者體驗及作業效率，成為關鍵。

一、暗黑模式之定義

各國主管機關近來注意到企業採取某些具有欺騙性的商業手段，可能導致消費者權益受到損害，尤其是網站所採取與使用者進行互動或溝通的介面，會推促、欺騙、迫使或操控使用者作出不符合使用者本身最佳利益的決定。為因應此議題，國際經濟合作組織(Organisation for Economic Cooperation and Development, 以下簡稱「OECD」)之消費者政策委員會，首度於2020年11月舉辦圓桌論壇，並於2022年10月依據論壇討論結果，發布「暗黑商業模式」此報告。該報告將暗黑商業模式(dark commercial pattern)定義為

*本文作者係創拓國際法律事務所資深顧問、臺灣與美國紐約州執業律師。本文感謝蔡采薇律師與國立台灣大學資訊工程學系博士班蕭皖文先生提供寶貴意見。

「此商業操作是使用有侵害或妨礙消費者自主性決策或選擇的數位選擇架構（digital choice architecture）——尤其是在網路使用者介面上。此通常欺騙、迫使或操控消費者，並很有可能導致消費者直接或間接在不同面向之損害，儘管該損害在很多情形下是無法或難以衡量」¹。

OECD指出暗黑模式用語的出現，最早源自使用者體驗設計師Harry Brignull在2010年，用以形容「網站或應用程式中讓使用者去做他本來無意要做的事的把戲，像是購物或報名活動」²。OECD將暗黑商業模式描述為企業經營者在數位環境中提供消費者在不同選項間進行選擇的流程或架構，而此流程或架構在與使用者溝通或互動的設計上，具有欺騙性、誘導或強迫性質，促使使用者反而無法做出合乎自己利益的選擇並可能承受金錢或精神上等損害。由此定義，可見OECD所使用暗黑商業模式，主要是針對網路科技對於商業活動帶來的影響——企業經營者能觸及更多消費者且更廣泛蒐集消費者線上活動紀錄，因此企業經營者可以運用資訊不對稱優勢並利用介面設計，發展出相較於實體環境對消費者權益影響更為顯著的作法。

二、暗黑模式的類型

就暗黑模式的具體內涵與樣態，可從其類型進一步觀察。OECD在2022年發布之暗黑商

業模式報告，將暗黑商業模式分為以下七大類型³：

- （一）**強迫採取動作（forced action）**：強迫使用者註冊或完成特定任務才能使用某種功能或服務，尤其是使用者被迫註冊，甚至是被迫揭露更多資料或被迫提供個人聯絡資料供業者從事行銷等。
- （二）**介面干擾（interface interference）**：利用介面設計讓使用者傾向採取對於業者較為有利的選項，例如預設選項、隱藏重要資訊、使用雙重否定語法結構的問題，或是將有利於業者的選項放在較前順位等。
- （三）**糾纏（nagging）**：持續推促消費者採取有利於業者本身運作的某些動作，例如開啟接收訊息通知或定位追蹤功能等。
- （四）**阻礙（obstruction）**：以消耗消費者意願或時間的方式讓消費者想要執行的動作變得麻煩或冗長，例如消費者自動被加入會員卻大費周章才能解除訂閱或變更成較為隱私友善的設定。
- （五）**隱匿（sneaking）**：隱瞞或延遲提供攸關消費者作出決定的資訊，例如在消費者挑選完商品要結帳時，才自動帶入無法取消或減免的費用，或是在未經消費者明確同意下在試用期屆滿

註1：OECD, DARK COMMERCIAL PATTERNS, October 2022, at 16,

https://www.oecd-ilibrary.org/science-and-technology/dark-commercial-patterns_44f5e846-en

註2：OECD, DARK COMMERCIAL PATTERNS, October 2022, at 8,

https://www.oecd-ilibrary.org/science-and-technology/dark-commercial-patterns_44f5e846-en

註3：Downloaded from

https://www.oecd-ilibrary.org/science-and-technology/dark-commercial-patterns_44f5e846-en

後轉為自動付費續約等。

(六) 社會認同效應 (Social proof) : 促使消費者在觀察其他消費者的行為後作出決定，例如通知該消費者其他消費者對於產品的回饋意見，但事實上其他消費者的購買時間可能並非近期紀錄而且意見也具有某程度誤導。

(七) 迫切 (urgency) : 例如透過設置具有誤導性的特價活動倒數計時器，營造時間緊迫或數量稀缺的急迫性，而給予消費者立即消費的壓力。

再者，歐盟執委會偕同由23個會員國主管機關組成之消費者保護合作網絡 (Network of Consumer Protection Cooperation, CPC network) 在2023年1月23日，共同發表其在2022年檢視399個零售電商網站的調查結果。此項調查鎖定電商網站常使用的三種操弄性作法 (manipulative practices)，也就是俗稱的暗黑模式 (dark pattern) ——這些作法通常會催促消費者做出其實不符合其最佳利益的選擇，包含虛假的倒數計時器、促使消費者點選購買或訂閱的網站設計，以及隱藏重要資訊或使消費者不容易發現特定資訊，像是運費、產品組成或有無其他較便宜的選項等。歐盟執委會調查範圍可粗略對應至OECD報告所指出之迫切、隱匿及界面干擾三大類暗黑

商業模式，調查結果顯示超過四成即高達148個網站使用至少其中一種模式⁴。

歐盟個人資料保護委員會 (European Data Protection Board，以下簡稱EDPB) 在2022年3月14日首次發布「在社群媒體平台介面中具有欺騙性的設計模式指引：如何辨識與避免」 (Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them，以下簡稱03/2022號指引)。在該指引中，定義「具有欺騙性的設計模式」為「社群媒體平台所導入的某些介面與使用者體驗，是在試圖影響使用者作出無意地、無意願或對其具有潛在危害決定。此類決定經常是不符合使用者最佳利益，反而在個人資料處理上是偏厚社群媒體平台」。此類具有欺騙性的設計模式，旨在影響使用者的行為、阻礙其有效保護個人資料的能力並做出有意識的決定。03/2022號指引將具有欺騙性的設計模式分為以下六大類型⁵：

(一) 過載 (overloading) : 使用者面臨雪片般襲來的大量請求、資訊或選項，而促使使用者在無意間分享更多個人資料或同意超出其預期的個資處理範圍。

(二) 省略 (skipping) : 透過介面或使用者體驗的設計，讓使用者忽略或未曾想到全部或部分個資保護面向。

註4：EU Commission, Consumer protection: manipulative online practices found on 148 out of 399 online shops screened, 30 January 2023, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418

註5：EDPB, Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them (Version 2.0), Adopted on 14 February 2023, at 3-4, https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

- (三) **擾動 (stirring)**：透過訴諸情感或視覺效果影響使用者的決定。
- (四) **阻礙 (obstructing)**：讓步驟變得更難或根本無法達到，而阻礙或防堵使用者在知情或管理個人資料的流程。
- (五) **善變 (fickle)**：操作介面的設計是不一致且不明確，導致使用者難以在不同的個人資料保護控制工具間進行切換，或掌握個資處理目的。
- (六) **蒙在鼓裡**：以隱瞞資訊或隱藏個資保護控制工具的方式設計介面，或讓使用者不確定資料如何被處理以及其當事人權利。

03/2022號指引使用「具有欺騙性的設計模式」，而非OECD所使用之暗黑商業模式，或是歐盟在其他政策文件所使用之暗黑模式⁶。首先，暗黑模式作為泛稱操控或誘使使用者有意無意作出有利於企業之決定或行為的介面設計，對於使用者權益的影響層面包含隱私與消費者保護兩層面，OECD與EDPB

雖同樣關注服務提供者試圖影響或控制使用者選擇之資訊溝通與互動介面設計，但兩者定義與類型界定有所差異，OECD放眼影響或削減消費者包含財務與隱私等權益且具有欺瞞性或誤導性之手段，而後者則著重在提供社群平台服務之個資控管者，如何透過介面與使用者體驗，影響當事人知情同意與行使當事人權利等與個資當事人控制其個資提供與否與利用範圍相關之決定。由於OECD與EDPB規範重心不同，因此其文件中界定「操控或影響消費者或使用者決定之介面、架構與使用者體驗設計」之類型，亦有不同。然而，個別類型間未必可以明確劃分。隨著網站產業活絡蓬勃、日新月異發展以及主管機關規管重心差異，使所謂暗黑模式的樣態幾乎不可能完全窮盡，亦難明確且完整定義。

部分主管機關並未直接使用暗黑模式此用語，例如英國資訊官辦公室與市場競爭主管機關競爭暨市場管理局於2022年共同發布「數位市場中有害的設計：線上選擇架構作

註6：歐盟執委會在2021年發布2021/C 526/01指引，針對不正商業行為指令（Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market），提供解釋適用之指引。該指引指出指令適用範圍涵蓋所有企業與消費者之間的交易，包含企業從締約前交易環境、廣告、交易履約到售後等各階段運用演算法、自動決策機制或人工智慧等科技與消費者互動的實務作法。該指引特別指出隨著科技運用，使得數位環境中大量消費者屬性、偏好及行為資料持續生成與累積，而企業透過資料可以依據個別消費者屬性提供客製化的廣告推播、推薦系統、定價等，而更有效地促成交易。該指引文件提及「暗黑模式」（dark pattern）一詞，用來指涉惡意推促的型態，通常結合數位介面設計。暗黑模式可以是基於資料導向、針對個別消費者資料所採取的差別設計，也可以是透過一班預設選項或行為偏見的設計，而達到操縱消費者的效果，視其具體操作是否有構成誤導或不正競爭手法，而有該指令適用。該指引文件並未就暗黑模式提供定義，但已指出某些咸認為暗黑模式的類型——例如隱藏商品服務重要資訊或錯誤引導消費者認為特定商品庫存有限或稀缺之操作方式，是不正商業行為指令之規範範圍。參Commission Notice 2021/C 526/01 - Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ%3AC%3A2021%3A526%3AFULL>

法如何消滅消費者對於個人資料的選擇與控制」⁷，英國個資保護與市場競爭的兩大主管機關即關注線上選擇架構（Online Choice Architecture）的設計問題——亦即數位環境中資訊與選項如何被呈現，影響消費者的決策與網路行為。該報告指出不佳的線上選擇架構作法可能讓數位服務消費者同意網站對於其個資的廣泛蒐集與分享，而導致消費者不堪其擾的收到廣告，或是削弱消費者的控制或自主權，讓消費者無從撤回同意或須面臨繁瑣的步驟，甚至是讓消費者須耗費龐大時間精力才能完成符合其偏好的隱私設定，該報告所關注的「有害的線上選擇架構設計」與EDPB在指引中使用「具有欺騙性的設計模式」，具有相當重疊。

綜上說明，暗黑模式是個概括而廣泛的用語，通常是描述服務提供者採用具有欺騙性、誤導性或建立在行為心理、預設或偏見上而操控使用者行為或決定的介面或體驗設計，但其操作定義或類型因應主管機關規範重心而有不同。隨著數位科技發展與網路服務普及，個資蒐集活動重心從實體環境逐漸轉移到網路空間，由於個資控管者在取得當事人同意做為其資料處理基礎上具有高度誘因，為促使個資當事人同意網站或數位服務提供者等個資控管者的個資蒐集活動，個資控管者可能透過「隱藏可以拒絕同意的選項，或透過版面設計凸顯特定選項」、「讓使用者在選擇拒絕同意提供資料上相當繁

瑣」、「讓使用者不知不覺甚至無緣無故同意個資蒐集」等方式，引誘、誤導或干擾當事人作出有利於個資控管者的決定。近來各國個資主管機關亦開始關注暗黑模式在知情同意介面設計、內容揭露或操作上的運用，並試圖界定構成暗黑模式之不當介面設計。因此本文以下從主管機關裁罰案例，爬梳歐盟個資保護法規下對於知情同意介面的規管立場與意見，作為臺灣業者拓展或銜接歐洲市場之參考。

貳、從比利時主管機關認定廣告產業標準組織違反GDPR談起

比利時個資主管機關（Belgian Data Protection Authority, APD）在2022年2月2日，以歐洲互動廣告協會（Interactive Advertising Bureau Europe）所開發之產業標準，即「透明暨隱私架構」（Transparency & Consent Framework，以下簡稱「TCF」），違反歐洲一般個人資料保護規則（General Data Protection Rule, GDPR）相關規定，裁處25萬歐元。雖然本案裁罰金額相較於其他案件並未特別高昂，但歐洲互動廣告協會作為重要產業標準組織，且在2018年起即積極在符合GDPR下建立產業資料交換規格，竟然遭到主管機關認定違反GDPR，難免波及遵循歐洲互動廣告協會所訂定規格與標準之會員夥伴與

註7：Information Commissioner's Office & Competition and Markets Authority, Harmful design in digital markets: How Online Choice Architecture practices can undermine consumer choice and control over personal information, <https://www.drcf.org.uk/siteassets/drcf/pdf-files/harmful-design-in-digital-markets-ico-cma-joint-position-paper.pdf?v=380506>

廣告產業上下游業者，因此此一裁罰決定，毋寧是在數位廣告產業界投下震撼彈。

一、數位廣告採購之即時競價機制

早期的網路廣告投放，通常是由廣告主與廣告代理商事與媒體平台（Publisher）簽署委刊單，約定刊載期間及版位，並提供廣告素材在刊載期間內上架，使用者瀏覽網頁時就會在該媒體平台看到廣告內容。然而，隨著科技日新月異，網路廣告趨向精準投放，廣告代理商若能越快鎖定該產品或服務的潛在受眾，就可以針對受眾投放客製化的廣告，不僅減少不必要的廣告預算支出，也能同時提高廣告轉換為交易的成效。在程式化購買廣告成為趨勢下，即時競價機制（Real-Time Bidding, RTB）成為受到青睞的交易方式。

即時競價機制的運作方式，例如使用者拜訪像是新聞網或是部落格時，代表廣告主或廣告代理商的多個行銷技術公司，會針對使用者預計瀏覽頁面上的廣告投放版位進行即時競價，競價勝出的行銷科技公司將可在競標版位投放自己合作廣告主的廣告內容，競價是針對特定使用者或裝置在特定時間存取的頁面，使廣告主不用在固定時段綁在固定版位。至於行銷技術公司是否參與競標以及出價，是由行銷技術公司所設定的演算法在極短時間內，依據該網站類型與使用者所在區域、屬性或先前瀏覽紀錄等資料決定。

在即時競價生態系中，主要參與者，包含(1)需求方平臺（Demand-Side Platform）、(2)廣告交換平台（AD Exchange）、(3)供應方平台（Supply-Side Platform）以及(4)媒體平台（Publisher）等角色。媒體平台會將版位位

置、大小、使用者裝置型號、裝置ID、位置及其他資料，透過供應方平台提交至廣告交換平台，此時需求方平台會透過其管理資料平台依據該資料，分析版位投放位置與對象，是否其廣告主或其代理商所鎖定的潛在受眾；若是，需求方平台就會進一步提出適當價位參與競標，並在廣告交換平台對該版位進行出價，廣告交換平台會決定何者出價最高並讓得標者投放其指定的廣告內容。

這一系列的運作是演算法與程式主導下之自動化交易，而能讓這自動化交易順利運作的重點，在於如何在不同平台間進行版位資料的判讀與拋轉。歐洲互動廣告協會所建立的TCF，就是旨在符合歐盟當地法規下，為促進線上廣告生態系統中這整個即時競價機制能夠運作的資料交換規格與技術標準。

二、網站基於廣告行銷目的取得使用者資料應經使用者明示同意

網站通常會使用自己本身的cookies，亦即第一方cookies，以記錄使用者在本身網站上的活動與登入資料；至於由第三方提供的cookies或其他追蹤技術，是網路廣告技術核心，媒體平台透過與第三方cookies合作，可以讓第三方cookies合作的廣告主在其頁面展開更多廣告投放與行銷活動。

歐洲法院對網站使用cookies是否需取得使用者同意，在2019年間作出明確見解。此爭議源自於德國電子商務網站Planet 49在2013年間舉辦網站抽獎活動，參加抽獎的使用者在輸入郵遞區號後會跳轉至輸入姓名與地址的頁面，此時頁面下方會出現網站聲明，載明「使用者同意網站使用cookies以用來評估

使用者瀏覽紀錄與網站活動並提供客製化廣告」等用語，並已預先勾選「同意」，導致使用者如果沒有特別採取動作，網站即可透過cookies蒐集其相關活動紀錄並作為廣告行銷使用。因此，本案爭議在於使用者網路位址資訊是否屬於個人資料，以及媒體平台能否以預設同意方式，取得當事人對於網站使用cookies蒐集處理使用者裝置與網路位址等相關資料的同意。

電子隱私指令（Directive 2002/58/EC）第5(3)條規定：「會員國應確保僅有當該使用者業經提供明確且完整的資訊且表示同意下，[服務提供者]才能儲存資料或存取已儲存於使用者終端設備的資料。但[服務提供者]基於在電子通訊網路進行傳輸之單一目的，而有技術性儲存或存取之必要時，不在此限」。歐洲法院在本案中依據前開規定，釐清網站經營者或服務提供者在網站頁面，以預先勾選同意欄位的方式取得使用者同意是否有效。

歐洲法院指出，電子隱私指令對於使用者如何表示同意，並無任何限制，只要是以適當方式表示使用者意願即可；然而，由於cookies會存取使用者網路位址，而網路位址屬於可得識別特定個人之資料，因此蒐集此類資料應得使用者同意之要件，參照當時適用之個資保護指令，須為「自由地提供、特定且經告知且沒有疑義地表示個資主體對於處理其個人資料之意願」，此「表示」須為個資主體明示表示，而非被動為之，因此網

站若以預設同意方式取得使用者同意，不構成所謂使用者明示表示。

回歸到本案爭議，歐洲法院認為Planet 49使用cookies是基於廣告目的，為其抽獎活動合作夥伴蒐集使用者資訊，歐洲法院重申該「同意」必須是針對特定個資處理目的所為同意，而不能以其他方式包裝、暗示，例如使用者點選「參加活動」不能代表已同意接受cookies。因此，網站除應明確告知使用者關於cookies運作期間、資料保留期間，以及資料是否分享予第三方及其他應告知之資訊，以確保使用者確實了解其所為「同意」的內容與範圍以外，更應讓使用者以明示方式表示同意，而不能以預設勾選同意方式為之⁸。此判決成為歐盟境內網站cookies政策或同意聲明此類通知介面設計之基礎。

三、同意聲明管理平台的興起與運作

歐洲互動廣告協會是針對歐洲數位行銷與廣告市場，藉由產業合作、提供相關架構與標準以促進市場發展的協會，會員包含5000多個各國產業協會組織與公司企業。為因應GDPR施行，歐洲互動廣告協會在2018年4月25日發布第1.1版TCF，歐洲互動廣告協會官方網頁上指出：「TCF是由產業為產業所打造的唯一GDPR同意方案…TCF的目標是協助所有夥伴在數位廣告產業鏈中，確保其處理個人資料符合GDPR與電子隱私指令」⁹。

由於即時競價機制運作過程中仰賴對於

註8：Case C-673/17, Judgment of the Court (Grand Chamber) of 1 October 2019, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62017CJ0673>

註9：IAB Europe, TCF, <https://iab europe.eu/transparency-consent-framework/>

使用者資料之交換與分享，因此TCF的重要角色之一為同意聲明管理平台（Consent Management Platform, CMP），由此服務提供者負責確認與記錄使用者是否同意分享其個人資料。同意聲明管理平台是負責開發cookies政策或類似通知內容，以告知使用者資料蒐集並記錄使用者對於可否蒐集處理其資料之偏好。同意聲明管理平台在遵循TCF政策下，應告知使用者的內容包含(1)讓使用者知悉該媒體平台採用的cookies或其他追蹤技術及其合作的廣告供應商、(2)讓使用者知悉並選擇是否接受個別資料利用用途，以及(3)以指定格式並以字串序列方式記錄使用者的選擇結果¹⁰。

實際運作上，當使用者拜訪歐盟境內運營的網站，該網站合作的同意聲明管理平台業者會先偵測使用者的網路位址、cookies或使用者裝置，以確認使用者先前是否已有既存設定，若CMP無法偵測到任何既有設定，CMP就會在使用者瀏覽器頁面呈現一則同意聲明（consent notice），並記錄使用者的回饋，隨後將此回饋依據產業標準轉為特定格式的TC字串（TC String），TC字串會傳送給該媒體平台合作之供應商，由供應商依據使用者同意範圍與對向，決定供應商有無權限投放廣告。

四、比利時主管機關認定TCF違反GDPR

自2019年起有多件針對歐洲互動廣告協會TCF運作違反GDPR合法處理、透明性及目的限制等原則的申訴案件，比利時個資主管機關（Belgian Data Protection Authority, APD）遂就TCF是否符合GDPR相關規定展開調查。

儘管歐洲互動廣告協會主張其僅作為技術標準組織、並未涉及個資蒐集處理，但主管機關認定，在歐洲互動廣告協會開發出的TCF下，同意聲明管理平台會存取使用者裝置資訊、確認使用者曾否與是否對於資料提供網站合作夥伴利用之同意與反對紀錄，並將此紀錄轉為特定格式編碼，雖然此段編碼本身承載資料有限，但主管機關認為同意聲明管理平台無可避免地會蒐集到使用者網路位址，而網路位址業經GDPR明確認定可得識別特定個人的資料¹¹。

比利時主管機關於2022年2月2日，在與其他歐盟會員國主管機關取得共識下，認定歐洲互動廣告協會在透過以編碼記錄使用者同意與否、選擇及偏好下，符合個資控管者之定義；另外，考量到資料處理的範圍與性質，同意聲明管理平台所提供給使用者的資訊過於廣泛且含糊，以致使用者難以控制資料流向。因此主管機關認定歐洲互動廣告協

註10：IAB Europe, TCF for CMPs,
<https://iabeuropa.eu/tcf-for-cmps/>

註11：“Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.”, Recital 30 of the GDPR,
<https://eur-lex.europa.eu/eli/reg/2016/679/oj>

會所開發建立之TCF不符GDPR原則，而裁罰25萬歐元¹²，此案經歐洲互動協會向比利時法院提出救濟，目前仍在審理中¹³。

比利時主管機關對於歐洲互動廣告協會的調查，多集中於網站是否在未經使用者同意且非基於網站服務所必要，使用cookies等網路追蹤技術蒐集使用者資料，以及網站不能以使用者概括同意服務條款或隱私權政策作為業經使用者同意而處理個資之基礎，主管機關重申分析或行銷等不同特定目的cookies的使用，應個別取得使用者同意¹⁴。然而，在比利時主管機關認為TCF運作有違反GDPR理由之一，是透過同意聲明管理平台介面提供給使用者的資訊，過於概括且空泛，無法讓使用者了解資料處理的性質與範圍，而且考量到TCF的複雜性，使用者後續難以控制其個人資料在網站合作供應商間的散布與利用。此案例某程度凸顯出個資控管者在導入新興應用技術時，如何在提高使用者接受度與讓使用

更簡易了解資料處理活動之介面設計兩難。

參、暗黑模式席捲下對於同意聲明管理介面設計的檢討

對於同意聲明管理平台或其背後的整體數位廣告產業而言，若同意聲明的介面設計能讓使用者直接點選「同意」，可使於網站合作的行銷技術夥伴取得使用者資料，而可以依據使用者屬性，更精確地在使用者瀏覽頁面上的廣告版位，投放符合使用者偏好或調性的廣告，以提升廣告效益。因此，同意聲明管理平台服務提供者具有改變此類同意聲明的介面設計的誘因，以盡可能讓使用者不知不覺、或無論基於何種原因點選同意。各國個資主管機關近來關注網站是否採用具有欺騙或誤導手段或介面設計，並檢討網站導入此類機制下取得當事人同意下所為資料處理對於使用者隱私消費權益及整體社會之影響。

註12：The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR,

<https://www.dataprotectionauthority.be/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr>

註13：歐洲互動廣告協會收到處分後，隨即於2022年3月針對主管機關裁處決定向比利時法院提出救濟，比利時法院於2022年9月針對該編碼機制是否涉及個資與歐洲互動協會是否因主導該技術標準而成為共同個資控管者兩大爭點，向歐洲法院聲請初步判決。歐洲法院於2024年3月7日作出裁定，表示若編碼含有任何識別碼而可連結至特定個人，諸如IP位址，就會構成個人資料；另外，若歐洲互動廣告協會本身對於資料處理目的與處理方式有某程度影響時，即與其會員構成個資控管者。因此，比利時法院需依歐洲法院上開兩點意見，就歐洲互動廣告協會的編碼格式是否屬於個人資料，以及歐洲互動廣告協會運作方式是否構成共同個資控管者兩點，進一步認定。Case C-604/22, JUDGMENT OF THE COURT (Fourth Chamber), 7 March 2024, POINT 77,

<https://curia.europa.eu/juris/document/document.jsf?text=&doid=283529>

註14：IV.7.2.1- Concerning the criteria for valid consent, at point 115-130, Decision on the merits 11/2022 of 21 January 2022,

<https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-11-2022-anglais.pdf>

一、被操縱的同意

有研究團隊在2019年9月間依據網路流量排名，調查前1萬個英國網站所合作同意聲明管理平台的介面設計，有以下主要發現：

- (一) 已導入同意聲明管理平台的網站中，有高達32.5%是採用默示同意，亦即當使用者有瀏覽網站、滑動頁面或點選頁面選項等行為時，即視同同意網站的隱私權政策。
- (二) 絕大部分的同意聲明管理平台將「全部拒絕」相較於「全部接受」更難找到，甚至只有12%的網站提供「全部拒絕」的選項。
- (三) 就算同意聲明管理平台有提供「全部拒絕」這選項時，同意聲明管理平台，也是以放在「全部接受」的下方或是點選進階頁面才能找到。

該研究進一步針對較不熟悉此類同意聲明介面的40位美國受試者進行實驗，以調查同意聲明管理平台的介面設計是否影響其選擇，實驗後發現若「全部拒絕」的選項沒有出現在介面第一層（first layer of user interface）時，有助於提高使用者同意的比例

達22-23%，此外若在同意聲明的第一層介面提供越細緻的選項，將導致同意的比例降低至少8%¹⁵。

從該研究所進行的實驗結果顯示，在介面設計上，若網站選擇不要在介面第一層提供「全部拒絕」的選項，以及選擇不要在介面第一層精細描述目的或利用方式的個別選項，而是僅以模糊概括的選項替代，可以促使同意聲明管理平台更高比例地取得使用者同意網站與其合作供應商處理其個人資料。這也某程度反映服務提供者可透過介面設計，潛移默化甚至具有欺騙性地利用使用者認知或慣習，獲取使用者同意的現象。

二、採用暗黑模式之知情同意介面構成違反GDPR之可能事由

歐盟個人資料保護委員會03/2022號指引指出與社群媒體平台介面設計攸關的個資法規遵循面向¹⁶，亦即當服務提供者以扭曲、具有欺騙性、刻意隱匿資訊或預設選項等暗黑模式，誘使使用者同意服務提供者的個資蒐集處理時，恐涉及GDPR以下規定之違反¹⁷：

(一) GDPR第5條第1項公平處理原則：本

註15：Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20). Association for Computing Machinery, at 5-9.

<https://doi.org/10.1145/3313831.3376321>。類似研究亦可參考Nataliia Bielova, Survey of academic studies measuring the effect of dark patterns on acceptance consent rate of users in consent banners, Study written in 2022 while working in the LINC team, CNIL, https://www.cnil.fr/sites/default/files/atoms/files/full_2022-12-02_v2.pdf

註16：Id., at 11-12

註17：本段以下GDPR中文翻譯，使用財團法人金融聯合徵信中心版本，可參考個人資料保護委員會籌備處，歐盟GDPR法規，下載自 <https://www.pdpc.gov.tw/CP/55/>

項明訂「個人資料應為資料主體為合法、公正及透明之處理」。該指引指出此原則可做為評估現行網站設計是否符合個資保護之起點，由於所謂「公允」的概念相當廣泛，包含個人資料不得以有害、歧視性、無預期、或對於個資主體具有誤導性的方式處理，因此若介面呈現資訊不足或有誤導性並符合「具有欺騙性的設計模式」的特性，應被認定屬於不正處理（unfair processing）而有違反情事。

（二）GDPR第12條第1項透明性原則：本項前段明訂「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條所定關於對資料主體所為處理之任何溝通」，GDPR前言第39點亦強調透明原則尤其關注於向資料主體公開控管者身分、其處理資料之目的及進一步資訊，且個人資料處理之特定目的應具明確性及合法性，且應於蒐集個人資料時告確定。因此，若介面呈現資訊有片段、隱匿、含糊，或刻意以長篇大論毫無邏輯方式提供告知事項，均有可能違反本項。

（三）GDPR第25條隱私保護機制導入設計原則：GDPR第25條第1項規定「考量到現有技術、執行成本以及處理之性質、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，不問係在決定處理方式時或係在處理中，控管者均應實施適當之科技化且有組織的措施，例如假名

化，且該等措施旨在實現資料保護原則，如資料最少蒐集原則，並採取有效方式且將必要保護措施納入處理程序，以符合本規則之要求並保護資料主體之權利」，課與個資控管者控管者個資活動規劃初始，應將必要的隱私保護機制納入個資處理流程設計之義務。因此若業者未妥善設計介面，以周延考量對於使用者個資保護之需求，而有使使用者被迫或無意間揭露更多個資時，即有違反本條情事。

在歐盟個人資料保護委員會提示可能用以處理暗黑模式問題之法規依據下，即有必要同步觀察會員國主管機關在此指引下之實際落實作為。

三、主管機關近期以業者使用暗黑模式違反GDPR之裁罰案

歐盟個人資料保護委員會03/2022號雖是針對社群媒體平台，但使用者介面與使用者體驗設計中的暗黑模式同樣見於一般網站，而受到歐盟會員國個資主管機關的重視。該指引歷經公眾徵詢程序而於2023年2月14發布第二版後，義大利個資保護主管機關旋於2023年2月23日，做出歐盟第一個直指暗黑模式違反GDPR之裁罰決定，而在2024年9月6日，比利時主管機關更進一步對於介面設計違反GDPR有更為具體之認定，顯見歐盟會員國主管機關嘗試回應該指引所提出的實務問題，而轉為更明確的執法標準。

（一）義大利：頻繁通知與未以相同方式提供對應選項之暗黑模式違反GDPR

Ediscom公司是透過簡訊、電子郵件及自動撥話等管道對顧客提供行銷活動的公司，依

據義大利主管機關調查結果，Ediscom在多個網站採用具有誤導性與欺騙性的介面，用以蒐集使用者對於收受行銷訊息的同意——包含使用者並未同意接受行銷訊息或同意將其資料提供給第三人從事行銷時，網站會持續以彈跳視窗取得使用者同意，而且彈跳視窗並未同時提供「讓使用者繼續既有流程而無庸同意」的選項，而是在網頁其他位置以不同格式、不同字體顯示拒絕同意行銷之選項。

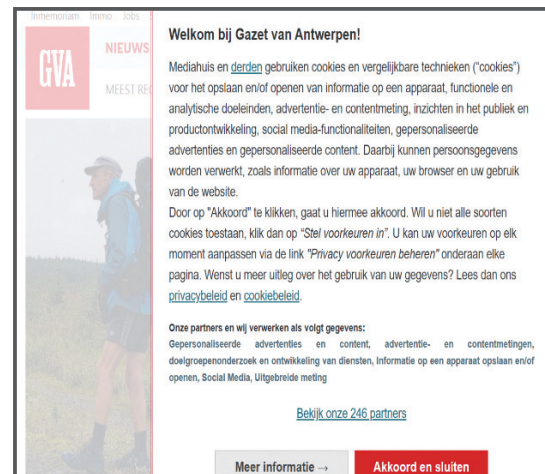
義大利個資保護主管關認定此介面設計違反GDPR第5條公平透明原則、第4條關於同意取得要件以及第25條隱私納入設計原則，有誘騙使用者同意個資控管者得基於行銷目的處理其個資的情事¹⁸。此處是歐盟會員國主管機關首見明確指出個資控管者以暗黑模式取得同意違反GDPR之案例，並裁處相當於Ediscom年營業額2%之30萬歐元。

Ediscom採用的暗黑模式，包含OECD定義下之糾纏、介面干擾及隱匿等類型。有學者指出該處分值得關注之處，不僅是主管機關在調查過程中，須保存網站頁面操作紀錄，因此處分書內容除文字敘述以外，尚輔以大量螢幕截圖，實屬罕見以外，主管機關亦相當具有突破性地認定Ediscom刻意將同意行銷與不同意行銷兩個具有對應關係的選項，用不同位置、字體與版面呈現給使用者，並非單

純隨機安排或錯誤設定，而是業者刻意透過介面設計，讓使用者無法直接選擇合乎其意願的選項，而讓使用者須耗費額外時間精力始能發現可能選項，進而影響使用者自主性與決定¹⁹。

(二) 比利時：同意與不同意選項應併列且分析或行銷cookies需經使用者同意

比利時個資主管機受理民眾舉發，發現由MediaHuis此公司經營的四個網站，其網站的cookies政策宣告介面的第一層，並未提供拒絕的選項，且MediaHuis對於選項採用不同顏色，具有誤導性。MediaHuis反駁表示GDPR並未明文要求個資控管者應在cookies使用政策第一層即提供拒絕選項，或應使用何種顏色顯示，故其做法就算未符合主管機關公告指引，亦不因此構成違反GDPR²⁰。



註18：IRIS Legal Observations of the European Audiovisual Observatory, The Italian Data Protection Authority adopts first decision on deceptive design patterns, 2023-6:1/13, <https://merlin.obs.coe.int/article/9784>

註19：Cristiana Santos, The emergence of dark patterns as a legal concept in case law, Internet Policy Review, <https://policyreview.info/articles/news/emergence-of-dark-patterns-as-a-legal-concept>

註20：APD/GBA (Belgium) -113/2024, September 6, 2024, [https://gdprhub.eu/index.php?title=APD/GBA_\(Belgium\)_-_113/2024&mtc=today](https://gdprhub.eu/index.php?title=APD/GBA_(Belgium)_-_113/2024&mtc=today)

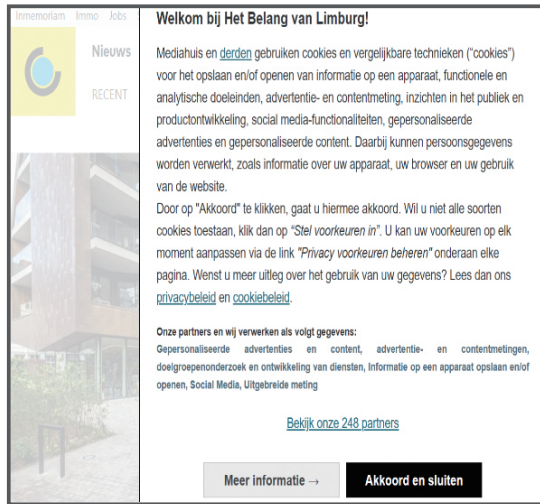


圖1：MediaHuis營運網站以彈跳視窗顯示之COOKIES政策²¹

比利時主管機關於2024年9月6日做出決定，指出「為確保使用者的同意，是在符合GDPR第6(1)(a)條與電子隱私指令第5(3)條規定下，自由且無疑義所為表示，拒絕的選項應該與接受的選項併同呈現，否則使用者在決定cookies設置與處理上，除同意以外，無從得悉實際上之替代方案」；其次，比利時主管機關認為個資控管者對於同意選項使用不同顏色，是具有誘導使用者同意cookies處理的性質，因此認定違反GDPR第5(1)條明定之公平合理原則。

最末，主管機關指出MediaHuis使用不同類型的cookies，包含分析功能的cookies此類非屬必要之cookies，依據電子隱私指令規定，若非屬於通訊所必要而有蒐集或存取使用者裝

置時，應經使用者同意，而個資控管者僅以具有合法利益作為個資處理依據，顯然違反GDPR第6(1)(a)條。因此主管機關針對上開違法事項，要求個資控管者應在45天內改善，若未改正，將依違規天數就每一網站裁處25,000歐元，累計上限至1000萬歐元²²。

四、歐洲互動廣告協會發布新版規範

歐洲互動廣告協會TCF工作小組在收到比利時主管機關裁罰後雖立即尋求救濟，但仍同步研擬因應方案，並在2023年5月23日發布TCF第2.2版，讓參與TCF此運作制度之成員，能夠更透明地讓終端使用者知悉TC字串處理情形，參與TCF的同意聲明管理平台服務提供者須於2023年9月30日前完成轉換並落實新版規範²³。新版規範主要調整方向如下：

- (一) 供應商基於廣告目的處理個資應取得使用者同意，而不得以合法利益為依據：原有第2.1版規範建立的特定目的列表，允許供應商得依據合法利益或使用者同意，基於「建立個人化廣告檔案」、「選擇個人化廣告」、「建立個人化內容檔案」及「選擇個人化內容」等四個目的處理利用使用者資料，但新版第2.2版要求供應商僅能在取得使用者同意下，始能基於此四個

註21：左圖為Gazet van Antwerpen，<https://www.gva.be/>；右圖為Het Belang van Limburg，<https://www.hbvl.be/> (last visited: 2024/9/21)

註22：APD/GBA (Belgium) - 113/2024, September 6, 2024, [https://gdprhub.eu/index.php?title=APD/GBA_\(Belgium\)_-_113/2024&mtc=today](https://gdprhub.eu/index.php?title=APD/GBA_(Belgium)_-_113/2024&mtc=today)

註23：IAB, TCF v2.2-Implementation FAQs, <https://iab europe.eu/tcf-faqs/>

目的處理使用者資料。

(二) 同意聲明管理平台介面資料揭露內容應更為完整：新版規範要求同意聲明管理平台提供的使用者介面第一層，應揭露擬尋求使用者同意或基於合法利益而擬處理資料之第三方供應商數量²⁴；另外，新版規範要求同意聲明管理平台使用者介面第二層，應將供應商相關資訊予以標準化，例如增加資料儲存類型與期間等說明，以利使用者進一步查閱²⁵。附帶說明，在TCF第2.2版問答集中，歐洲互動廣告協會指出儘管新版政策並未要求同意聲明管理平台將拒絕選項置於使用者介面的第一個畫面，但該標準從未禁止同意聲明管理平台可提供優於標準的設計。

以歐盟境內重要媒體網站導入之同意聲明管理平台現行操作介面為例，使用者首次拜訪該頁面時，該網站頁面會出現cookies政策彈跳通知，關於其三層介面設計分別說明如下：

(一) 第一層：詢問使用者是否接受該網站與其共計864個合作夥伴所使用之cookies或類似技術，畫面上方告知使用者可毋庸同意並繼續使用網站服務，畫面下方有兩個選項，左邊是「了解更多」，右邊藍底選項是「同意並關閉」。當使用者點選「同意並關閉」。

時，該畫面就會關閉並記錄使用者同意分享其個資給該網站及其合作夥伴。

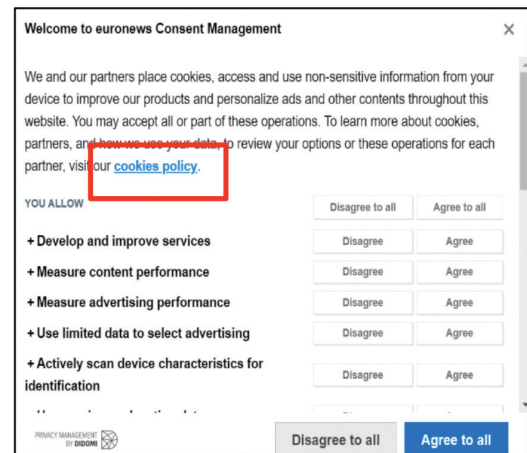
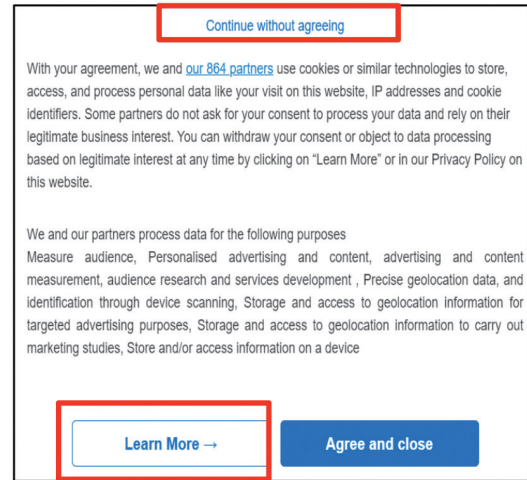


圖2：同意聲明管理平台介面之第一層與第二層畫面截圖

(二) 第二層：點選第一層介面畫面下方「了解更多」後會進入第二層，第二層畫面上方概略說明cookies使用需求，並提供使用者連結至完整版說明，可瀏覽所有供應商cookies名稱、屬性及運作期間；畫面主要內容則是臚列網

註24：IAB, TCF v2.2-Implementation FAQs, <https://iabeuropa.eu/tcf-faqs/>

註25：IAB, Understanding the Transparency & Consent Framework v2.2, 24 June 2023, <https://iabeuropa.eu/understanding-the-upcoming-transparency-consent-framework-v2-2/>

站與其合作夥伴共計10多個資蒐集目的，例如「開發與改善服務」、「評估內容效益」、「評估廣告效益」、「使用有限資料以挑選廣告」或「主動偵測裝置特性作為識別」等目的，使用者可以個別選擇拒絕或接受，或直接點選全部拒絕。

ADVERTISING COOKIES
These cookies are placed by advertisers. If you give your consent, personalised ads can be shown to you based on your profile (country, browsing history...), in order to get more relevant ads and offer a personalised experience. The performance and effectiveness of ads that you see or interact with can be measured.

PARTNER	COOKIES	USAGE	PERSISTENCE
Audience Manager	adm_uidid	Set for ID sync for Adobe Audience Manager	1 month
	demdex.net	The demdex cookie helps Audience Manager perform basic functions, such as visitor identification, ID synchronization, segmentation, modeling, reporting, and so on.	6 months
Adara	fbid gma rmxc okst okst dph ph	Provides advertising or advertising related services such as data collection, behavioral analysis or retargeting.	1 year
Rombox		Second party data. Data Enhancement : convert unknown audience using E2B	1 year

Welcome to euronews Consent Management

- + Create profiles to personalise content Disagree Agree
- + Use profiles to select personalised advertising Disagree Agree
- + Create profiles for personalised advertising Disagree Agree
- + Store and/or access information on a device Disagree Agree
- + Measure audience **REQUIRED**
- + Storage and access to geolocation information for targeted advertising purposes Disagree Agree
- + Storage and access to geolocation information to carry out marketing studies Disagree Agree
- + Use limited data to select content Disagree Agree

By giving consent to the purposes above, you also allow this website and its partners to operate the following data processing: Deliver and present advertising and content. Ensure security, prevent and detect fraud, and fix errors. Identify devices based on information transmitted automatically. Link different devices. Match and combine data from other data sources, and Save and communicate privacy choices

+ About the storage of your choices

圖3：同意聲明管理平台介面之第二層提供cookies完整政策連結，該政策提供供應商使用的cookies清單，使用者可檢視個別cookie屬性與運作期間

(三) 第三層：介面第二層的畫面拉到最下方，會出現「檢視我們的合作夥伴」（view our partner）選項，點選進去進到介面第三層。使用者可以

檢視該網站合作的完整合作夥伴清單，亦即廣告供應商或行銷科技公司列表，使用者可以全部接受或拒絕，亦可個別決定封鎖或同意將資料提供給特定合作夥伴。

Select partners for euronews

You can set your consent preferences for every partner listed below individually. Click on a partner name to get more information on what it does, what data it is collecting and how it is using it.

All partners	Block	Authorize
+ Apester Ltd IAB TCF	<input type="button" value="Block"/>	<input type="button" value="Authorize"/>
+ Applier PTE Ltd IAB TCF	<input type="button" value="Block"/>	<input checked="" type="button" value="Authorize"/>
+ Appmonsta Ltd IAB TCF	<input type="button" value="Block"/>	<input type="button" value="Authorize"/>
+ AppsFlyer	<input checked="" type="button" value="Block"/>	<input type="button" value="Authorize"/>
+ Appush Technologies IAB TCF	<input type="button" value="Block"/>	<input type="button" value="Authorize"/>
+ Arago IAB TCF	<input type="button" value="Block"/>	<input type="button" value="Authorize"/>
+ Arcanor Bilgi Teknolojileri ve Hizmetleri A.Ş. IAB TCF	<input type="button" value="Block"/>	<input type="button" value="Authorize"/>
+ Archon Programmatic House FZC IAB TCF	<input type="button" value="Block"/>	<input type="button" value="Authorize"/>

+ View user information

Euronews/Africanews

The present Cookie Policy applies when you consult the websites of Euronews, namely Euronews.com, Africanews.com, and our applications. ("our Websites" or "our Applications"). As explained in this Cookie Policy, you can manage your cookie choices at any time in the Consent management Platform (CMP) by clicking [here](#).

1. What's a cookie?
A cookie is a small piece of text sent to your terminal (computer, tablet, smartphone, etc.) by our Websites that you visit thanks to your browser.
Cookies deposited on your terminal can only be read by its issuer who is able, during their period of validity, to recognize your terminal each time you access digital content containing cookies from the said issuer. A cookie does not identify you personally, but only the browser on your terminal. Your browser will keep it for a certain period of time, and will send it back to the web server each time you reconnect to it.
When you use our Applications, an identifier of your mobile phone or tablet may be sent to us depending on the preferences you have expressed in your mobile phone or tablet, to track certain activities for advertising purposes.

圖4：同意聲明管理平台介面之第三層提供合作夥伴清單，若屬遵循TCF之IAB會員會在廠商名稱後加註；使用者若同意將資料提供給該供應商，則點選授權，圖框會轉為綠色，若選點封鎖，圖框會轉為紅色。若想變更此介面之任何設定，則可進入cookies政策之CMP頁面重新調整

從上開同意聲明管理平台介面，顯示歐洲

互動廣告協會主到之TCF規範因應主管機關規管立場所作調整，介面第一層讓使用者可以選擇同意，但同時提供使用者不作出同意下繼續網站服務之選項，符合近來歐盟個人資料保護委員會認為「不應迫使使用者點選同意始能使用服務」之立場，以及義大利與比利時主管機關認為選項應併陳置於同一版面之要求；其次，為提升比利時主管機關要求之TCF資料處理活動透明性，同意聲明管理介面第二層與第三層介面除提供簡要說明以及個別選項以外，並以超連結方式讓使用者可以檢視網站完整版本隱私權政策，而揭露個別cookies屬性與運作期間。

在比利時主管機關於2022年2月2日認定歐洲互動廣告協會所制定之TCF認有違反GDPR後，歐盟個人資料保護委員會於同年3月發布03/2022號指引，大幅影響TCF介面設計與資訊揭露作業之方向。此外，義大利與比利時個資主管機關相繼於2023年2月與2024年9月作出採用暗黑模式之使用者介面違反GDPR，對於介面設計有更明確的方向與界限，TCF此一產業標準是在歐盟規管立場從警覺、摸索而趨於嚴格的歷程中進行修正，因此其新版規範修正背景與初步結果對於使用者介面設計如何避免落入暗黑模式，有相當參考價值²⁶。

肆、未來展望

本文主要探討是主管機關在個資法制下對於網站採用暗黑模式以取得使用者同意之因應，尤其是對於網站使用cookies通知之規範。在因應高度競爭的網路環境中，企業無不發展能夠更快速達成交易、或提高行銷頻率或其他收益的機制，例如蒐集使用者網路位址與瀏覽紀錄以將客製化廣告推播給屬於廣告目標受眾之使用者等。姑不論知情同意做為資料蒐集基礎有其侷限²⁷，這些機制或設計本質上並不違法——若企業確實有向使用者揭露充分而完整之資訊，且給予消費者自由且公平決定或選擇的餘裕。

暗黑模式泛指不同類型且侵擾程度不一之欺騙性或誤導性的介面設計，暗黑一詞或許有某程度影射或強調「個資控管者對於取得使用者同意之手段，需具備某程度意圖或故意」。然而，從GDPR解釋適用而言，無論資料控管者對於此設計是否有預期其結果將侵害個資當事人權益或顯出於不正當之目的，均無法迴避其在蒐集處理個人資料上所應遵循之義務。歐洲法院、歐盟個人資料保護委員會及會員國主管機關，已針對cookies使用政策等類知情同意介面之設計，逐步明確界

註26：比利時主管機關裁處歐洲互動廣告協會TCF違反GDPR時，同時要求其在六個月內提出改善方案，歷經雙方溝通後，主管機關迅速於2023年1月核准歐洲互動廣告協會所提出方案並要求其於6月內落實。然而，比利時法院仍須依歐洲法院在2024年3月之初步裁決結果，實際認定歐洲互動廣告協會在TCF下是否屬於個資共同控管者以及TC字串是否屬於個人資料，因此歐洲互動廣告協會對於改善方案是否須落實仍持保留態度，認為仍應交由歐洲法院作最終判斷，但就此部分可能主要影響TCF中個資處理目的呈現與是否同意聲明管理平台是否在個資蒐集主體中列出歐洲互動廣告協會。

註27：參張陳弘（2018），〈新興科技下資訊隱私保護：告知後同意原則的侷限性與修正方法之提出〉，《台大法學論叢》，第47卷第1期。

定構成暗黑模式情事而有違法蒐集個資之界線，首先依據電子隱私指令，非屬服務所需而需存取或儲存資料於使用者裝置時，均須取得使用者同意，亦即當網站使用分析或行銷等非屬必要之cookies時，應取得使用者明示表示同意，網站不能僅基於具有本身營運考量之合法利益作為蒐集使用者網路位址與瀏覽紀錄之依據，且網站不能以顯著差異的色塊、或預設同意方式誘使使用者為同意，甚至應以適當方式，將「不同意」的選項併列，以讓使用者能夠更簡單而快速地了解替代選項，不能隱匿或以其他方式讓使用者難以選擇「拒絕」之選項。此外，從TCF新版規範，亦可發現業者在遵循GDPR下，如何透過介面設計，讓使用者能更審慎決定個別特定目的與了解cookies運作期間。

其次，暗黑模式是泛指影響使用者決定之選項架構、介面或使用者體驗設計，但由於暗黑模式類型繁雜且程度不一，並非採取暗黑模式即有違反GDPR，而應視該暗黑模式實際上是否影響使用者認知、理解與權利行使。再者，具有誤導性或欺騙性的網站介面所涉議題，並非僅有使用者隱私或個資保護，部分法規禁止此類做法，是基於保護網路平台使用者權益或維護產業公平競爭之考量。例如2022年11月16日通過之歐盟數位服務法

(Digital Service Act)對於網路平台與中介者等服務提供者課與義務，受該法規範之服務提供者須要評估其介面對於使用者的透明性與公正性，該法前言定義暗黑模式為「在網路平台介面中的暗黑模式，是刻意或就其結果而言嚴重扭曲或損害服務接收者做出自主且知情決定的作法」，包含濫用選項設計以指示服務接受者採取有利於網路平台服務提供者但不符合服務接受者利益之行動。該法第25條第1項禁止網路平台以欺騙、操縱或其他嚴重扭曲或損害服務接收者做出自由且知情決定之方式，從事介面設計²⁸。另歐盟於同年通過之數位市場法(Digital Market Act)則對超大型網路平台即守門員課與類似義務，該法第13條禁止此類平台透過結構、設計、功能或使用者介面運作方式或其部分，以不中立或影響終端使用者或企業使用者、自主性、決定及選擇的方式提供選項，甚至於前言中明確要求此類平台應給予使用者如同同意般同樣簡便之退出機制，不應以欺騙性、操縱性或嚴重損害使用者自由行使同意之方式設計、組織或運作其網路介面，當使用者未同意此類平台的處理目的或事後退出或撤回同意時，平台最多只能一年重新徵詢一次²⁹。因此，平台從事介面設計時，仍須注意其他法規所課與之義務或限制，當網站在

註28：Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance), <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>

註29：Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJL_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC

與使用者溝通互動以取得某些資料授權的介面上採取暗黑模式時，不僅有違反GDPR疑慮，依據網站服務提供者規模與屬性，仍有可能涉及其他規範或有構成廣告不實³⁰。

最末，歐盟近年逐漸累積實務案例，部分

介面設計原則已受到歐盟會員國主管機關肯認，因此我國業者若經營網站或提供數位服務，即須注意在台灣與歐盟在同意取得要件之差異下，進行cookies使用政策此類同意聲明管理介面之調整與銜接。我國主管機關肯

註30：例如英國資訊官辦公室與市場競爭主管機關競爭暨市場管理局於2022年共同發布「數位市場中有害的設計：線上選擇架構作法如何消減消費者對於個人資料的選擇與控制」報告。這兩個分別為英國個資保護與市場競爭的主管機關指出線上選擇架構（Online Choice Architecture）——亦即資訊與選項如何被呈現，影響消費者的決策與網路行為，不佳的線上選擇架構作法可能讓數位服務消費者同意網站對於其個資的廣泛蒐集與分享，而導致消費者不堪其擾的收到廣告，或是削弱消費者的控制或自主權，讓消費者無從撤回同意或須面臨繁瑣的步驟，甚至是讓消費者須耗費時間與精力查閱資訊或完成符合其偏好的隱私設定。不佳的線上選擇架構不單只是造成消費者不悅、不便或反感，長久以往將消費者置於此脆弱地位，讓消費者更難掌控其個人資料利用範圍與目的下，亦可能衍生金錢損失等財物損害，因此主管機關針對暗黑模式性質與影響，分別從個資與消費者保護法規——例如廣告不實等法令，釐清因應與處理方向，參Harmful design in digital markets: How Online Choice Architecture practices can undermine consumer choice and control over personal information, A joint position paper by the Information Commissioner's Office and the Competition and Markets Authority

https://www.drcf.org.uk/__data/assets/pdf_file/0024/266226/Harmful-Design-in-Digital-Markets-ICO-CMA-joint-position-paper.pdf。值得注意的是，英國競爭暨市場管理局在2022年11月對於床墊公司Emma Sleep的網路銷售活動展開調查，包含其採用倒數計時器、限時折扣及標示銷售快速等造成消費者壓迫感的方式，是否有誤導消費者情事。主管機關調查發現其產品雖標榜特價中，但實際上並未為消費者節省支出。另外，該床墊公司提供的網路商品折扣通常會伴隨倒數計時器，顯示該特價活動即將結束，但主管機關調查發現當一個特價活動結束後，就會被另一個特價活動取代，中間間隔甚至不到24小時，因此主管機關認為這樣的倒數計時器讓消費者誤以為商品在活動結束後就會回復原價，導致消費者在不想錯過特價活動的時間壓力下匆匆下單購買。因此，英國競爭暨市場管理局於2023年7月7日向Emma Sleep通知其操作方式有違反消費者保護法之疑慮並要求採取改正措施，參Competition and Markets Authority, Emma Group: consumer protection case, <https://www.gov.uk/cma-cases/emma-group-consumer-protection-case>；另外，美國聯邦貿易委員會在學習時代公司（Age of Learning, Inc.）案件，認定該兒童線上教育學習網站在2015年至2018年間使用具有欺騙性手法，包含(1)未明確告知會員資格會無限期地自動續約並持續寄發帳單給使用者、(2)強調解約手續簡便，但實際上卻製造讓使用者難以解約的障礙、(3)在解約流程中讓使用者誤以為解約，但使用者持續收到帳單才發現是展延會員資格等，而有違反FTC ACT與Restore Online Shoppers' Confidence Act（ROSCA）等情事。FTC最終與學習時代公司達成和解，且學習時代公司承諾將改善其不當作法，聯邦貿易委員會委員Rohit Chopra隨後針對此案所涉及的商業模式發表意見，首度以暗黑模式形容此手法並定義為「用來欺騙、引導或操弄使用者作出讓線上服務獲利，但通常損害使用者本身利益的設計特性」，暗黑模式運用技術與設計創造出讓使用者易進難出的陷阱。Rohit Chopra表示「聯邦貿易委員會有不少工具可以將這陷阱或花招根除」，例如部分法規要求企業經營者須明確揭露重要條款、禁止使用具有欺騙性的郵件主旨並須提供使用者退出收信名單的機制等，並強調聯邦貿易委員會應通盤應對違法的數位暗黑模式，參STATEMENT OF COMMISSIONER ROHIT CHOPRA, Regarding Dark Patterns in the Matter of Age of Learning,

認網路位址屬於個人資料³¹，因此網站服務提供者蒐集此類資料即須具有個資法第15條或第19條所定合法處理之任一事由，若網站基於履行資料傳輸服務所必要，應得基於「與當事人有契約或類似契約之關係，且已採取適當之安全措施」此事由作為蒐集依據，但若網站蒐集處理使用者個資之目的，與履行契約無合理關連，例如透過行銷或分析屬性之cookies將使用者資料提供給第三方投放廣告時，應須以當事人同意此事由作為蒐集依據較為適當。然而，我國個資法第7條第2項規定同意之方式，包含「公務機關

或非公務機關明確告知當事人第八條第一項各款應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已…表示同意」之推定同意，因此網站若以單純使用者繼續使用並被動提供資料之行為認定有同意之意思，恐與歐盟實務採取之明示表示不符³²。鑒於GDPR有域外適用效力，若我國業者有鎖定歐盟市場或對於歐盟境內使用者有資料剖析側寫或網路活動追蹤而有適用GDPR時，建議仍應審慎考量近來歐盟主管機關規管趨勢，調整或改善知情同意之介面設計。

Inc., September 2, 2020,

https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_rchopra_statement.pdf

註31：國家發展委員會發法字第1090015912號指出：「我國個資法主要係參考歐盟1995年個人資料保護指令（下稱95指令）制定，關於個人資料之定義亦與95指令相仿。參考歐洲法院（CJEU）2016年判決（Case C-582/14）亦明確指出，所稱「個人資料」，並未要求所有足使特定資料主體被識別之資料都必須由同一人掌握，例如保有動態IP位址（dynamic IP address）資料之服務提供者得以可能、合理之方式，透過其他網路服務提供者取得對照、組合之資料識別特定資料主體，即可認定動態IP位址屬於個人資料」，參個人資料委員會籌備處，

https://www.pdpc.gov.tw/News_Content/102/355/

註32：主管機關曾以函釋指出：「參照法務部98年1月8日法律字第0970038035號函釋意旨『當事人不同意提供利用，並無以書面簽名表示不同意之義務』，本件若欲符合推定同意要件之「當事人未表示拒絕」，應係當事人在正面選擇同意與否之模式下進行（例如：上開畫面宜顯示「提供定位資訊」），否則有類似「預設同意」效果之虞。至於本件若欲符合推定同意要件之「當事人已提供其個人資料」，應係指當事人有自行提供個人資料之積極行為（例如：自主開啟藍芽設定並選擇同步資料，並將資料傳送予業者）；倘業者預設自動上傳資料之功能，在當事人未有任何積極行為之情形下即取得個人資料，則縱使當事人未表示拒絕，仍不得視為當事人已提供其個人資料，因此應不符合推定同意之要件」，主管機關似嘗試釐清所謂推定同意之實務操作方式，主要是排除預設同意。參國家發展委員會發法字第1072002136號，

https://www.pdpc.gov.tw/News_Content/102/411/