

社群媒體平台可能違反歐盟 GDPR 透明度規定之黑暗模式

楊和潤 編譯

摘要

歐盟資料保護委員會於今 (2022) 年 3 月 21 日發布「一般資料保護規則」關於在社群媒體使用黑暗模式規範之指引草案，並於同年 5 月 2 日前開放公眾諮詢。該指引草案為社群媒體平台的設計者及使用者提供一實用準則，以辨別及避免於平台上使用可能違反歐盟「一般資料保護規則」之黑暗模式。其首先定義及分類何謂黑暗模式，並說明黑暗模式可能涉及之「一般資料保護規則」規定，接著依照社群媒體五個生命週期，舉例說明在各階段可能違反該規則之黑暗模式態樣。本文礙於篇幅，且因透明度作為「一般資料保護規則」之重要規範，對於檢視黑暗模式之合法性具有關鍵意義，故擬以透明度規範為核心，探討社群媒體平台中涉及透明化規定違反疑慮之黑暗模式事例。由於非從事社群媒體業務的公司，也可能因其於社群媒體平台所從事的商業行為落入黑暗模式的定義與態樣，從而引發歐盟隱私機構的審視，此等歐盟政府對資料保護更廣泛介入的趨勢，日後如何發展，值得持續關注。

(取材資料：Nicholas Shepherd & Dan Cooper, *EDPB Publishes Draft Guidelines on the Use of “Dark Patterns” in Social Media Interfaces*, INSIDE PRIVACY (Mar. 23, 2022), <https://www.insideprivacy.com/data-privacy/edpb-publishes-draft-guidelines-on-the-use-of-dark-patterns-in-social-media-interfaces/>.)

在今 (2022) 年 3 月 14 日舉行的歐盟資料保護委員會 (European Data Protection Board, EDPB) 全體大會之後，EDPB 在同年 3 月 21 日發布一份有關在社群媒體平台使用黑暗模式之指引草案 (Guidelines 3/2022 on Dark patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them)¹。該指引之目的是為社群媒體平台的設計者及使用者提供一實用準則，以辨別並避免於平台上使用可能違反歐盟「一般資料保護規則 (General Data Protection Regulation, GDPR)」之黑暗模式²。

該指引草案不僅指導公司如何以符合 GDPR 的方式設計其平台及使用者介

¹ European Data Protection Board [EDPB], Guidelines 03/2022 on Dark Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them, Version 1.0, Adopted on 14 March 2022, https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf [hereinafter Draft Guideline].

² *Id.* at 2.

面，亦教育使用者所面臨的哪些情況實際上可能違反 GDPR 規定³，從而增加使用者就違反 GDPR 之黑暗模式行為提出的控訴案件。指引草案於今年 3 月 21 日至 5 月 2 日屬於公眾諮詢的階段，目前則已結束⁴。

以下先介紹本指引草案中黑暗模式之定義及類別，再簡介黑暗模式可能涉及違反之 GDPR 規定，接著舉例說明可能違反 GDPR 透明度要求之黑暗模式態樣，最後以未來可能的影響作為結論。

壹、黑暗模式之定義及類別

指引草案將「黑暗模式」定義為「在社群媒體平台中會導致使用者就其個人資料的處理做出非預期、非自願與有潛在危害決定的任何介面和使用者體驗」⁵，並指出 6 種黑暗模式的類型，分別為⁶：

一、超載 (Overloading)：以提出大量請求、資訊、選項或可能性等方式，讓使用者無法在短時間內消化，促使他們分享更多資料。

二、跳過 (Skipping)：以易導致使用者忘記或未能充分考慮其有關全部或部分資料保護之決定的方式，設計介面或使用者體驗。

三、擾動 (Stirring)：訴諸使用者的情緒或使用視覺暗示的方式，影響使用者可能做出的決定。

四、阻礙 (Hindering)：藉由讓某些行動變得困難或無法完成，以阻礙或阻止使用者知悉其資料的使用情況、或妨礙其控制其資料。

五、反覆 (Fickle)：以不一致及不清楚的方式設計介面，讓使用者難以瀏覽不同的控制選項或了解資料處理的目的。

六、隱瞞 (Left in the dark)：以隱藏資訊、隱私控制選項、或讓使用者不確定其可以控制的選項以及其資料是如何被處理等方式設計介面。

貳、黑暗模式可能違反之 GDPR 規定

首先，EDPB 揭舉數個 GDPR 的基本原則，讓有意（與試圖避免）使用黑暗

³ *Id.*

⁴ *Public Consultation on Our Guidance: Guidelines 03/2022 on Dark Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them*, EDPB, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en (last visited June 10, 2022).

⁵ Draft Guideline, *supra* note 1, at 2.

⁶ *Id.* para. 5.

模式的公司和使用者得以依循：

一、公平及透明度 (GDPR 第 5 條第 1 項 a 款)

EDPB 強調 GDPR 的公平原則有「如同保護傘般的作用」，以防止個人資料被以有害、歧視、誤導或未預見的方式處理⁷。而關於透明度，根據 GDPR 第 12 條，資料控制者必須以「簡潔、透明、可理解及易於近用的形式，並使用清楚易懂的語言」向資料主體提供資訊。此為檢視黑暗模式是否違反 GDPR 規定的關鍵考量因素⁸。

二、資料控制者須負擔合規之舉證責任 (GDPR 第 5 條第 2 項)

EDPB 表示，相較於社群媒體使用者而言，社群媒體平台上的使用者介面／旅程本身，便可作為證明業者遵守 GDPR 相關規定之一種方式⁹。值得注意的是，EDPB 鼓勵社群媒體平台的營運商進行質性及量化研究 (例如 A/B 測試、眼動追蹤及使用調查)，並記錄介面截圖，以展示他們如何充分滿足 GDPR 的相關要求¹⁰。

三、設計與預設對隱私之保護 (GDPR 第 25 條)

EDPB 指出，基於 GDPR 第 25 條之規定，資料控制者在設計介面時必須考慮特定因素，以確保在設計過程中對隱私之保護，以及隱私選項之預設是有效的。特別是尊重資料主體的自主權與合理期待、使資料主體能夠輕鬆互動及行使權利、促進消費者的選擇權及避免權力不平衡，並以客觀中立的方式提供資訊，而非欺騙、操控或誤導資料主體¹¹。

本文由於篇幅，以下僅聚焦於探討可能違反 GDPR 透明度要求之黑暗模式的態樣，蓋透明度為上述指引文件提及在檢視可能的黑暗模式是否違反 GDPR 規定時之關鍵考量因素。

⁷ *Id.* para. 8; 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, art. 5(1), 12, 2016 O.J. (L 119) 1, 35 [hereinafter GDPR].

⁸ Draft Guideline, *supra* note 1, para. 14; GDPR, *supra* note 7, art. 12.

⁹ Draft Guideline, *supra* note 1, para. 11.

¹⁰ A/B 測試係指一種透過分析介面設計來優化使用者體驗的測試方法，其透過分析兩組介面設計來更科學化地了解使用者體驗。進行 A/B 測驗時會設計兩款介面分別為實驗組及對照組，當使用者使用網頁時會分別進入兩種不同的版本，而每位使用者在網頁內的動作都會被監控並記錄下來，以幫助設計者了解哪個版本使用者的點擊意願最大。Ryan，【硬塞科技字典】什麼是 A/B Testing，關鍵評論網媒體集團，2016 年 6 月 30 日，<https://www.inside.com.tw/article/6652-what-is-a-b-testing>；Draft Guideline, *supra* note 1, para. 11; GDPR, *supra* note 7, art. 5(2).

¹¹ Draft Guideline, *supra* note 1, para. 16; GDPR, *supra* note 7, art. 25.

參、可能違反 GDPR 透明度規定的黑暗模式態樣

依 GDPR 第 12 條第 1 項的透明化要求，資料控制者應採取適當的措施並依一致、透明、易懂且易於近用的形式，以清楚且簡潔的詞句提供 GDPR 所要求之相關資訊¹²。該些資訊應以書面的方式提供，在適當情況下亦可以電子方式提供之，然只有在資料主體要求且其身分已經由其他方式證明時，該些資訊始得以口頭的方式提供¹³。

按 EDPB 將社群媒體使用者帳戶的生命週期分為以下五個階段：一、開設社群媒體帳戶；二、保持受到通知的權利；三、在社群媒體上保持受保護的狀態；四、在社群媒體上行使個人資料相關權利；五、刪除社群媒體帳戶¹⁴。以下依各階段列舉指引草案中之例子，說明在各階段中可能違反透明度要求之黑暗模式設計。

一、開設社群媒體帳戶

當使用者在電腦瀏覽器上註冊社群媒體帳戶時，可能被邀請同時使用該社群媒體之手機應用程式，然而在點擊相關連結後，使用者卻被要求提供手機號碼以接收含有安裝該應用程式連結之文字簡訊¹⁵。

在此案例中，使用者對點擊連結之預期應是可直接下載應用程式、或被導引至應用程式商店中的安裝頁面，理應不需要透過寄送下載連結至使用者手機此種迂迴的方式。資料控制者很可能只是為了獲得更多的個人資料而選擇這樣的「阻礙」黑暗模式。

二、保持受到通知的權利

在社群媒體中，多有類似「你的資料可能會被我們用來增進我們的服務」此種隱私政策聲明¹⁶。此種聲明表面上事先告知使用者其資料可能會被資料控制者作為增進社群媒體服務之用，給予使用者評估是否使用該社群媒體之機會。然而，「可能」及「服務」此種模糊的用字，將導致使用者無法確定自己的資料究竟會不會被用來作上述處理、如何被處理、又是用於增進何種服務¹⁷。資料控制者上述之作法很可能構成「隱瞞」之黑暗模式¹⁸。

¹² GDPR, *supra* note 7, art. 12(1).

¹³ *Id.*

¹⁴ Draft Guideline, *supra* note 1, para. 1.

¹⁵ *Id.* para. 37.

¹⁶ *Id.* para. 67.

¹⁷ *Id.* para. 68.

¹⁸ *Id.*

三、在社群媒體上保持受保護的狀態

在瀏覽社群媒體動態頁面時，使用者有時會看到意外的廣告內容，而這些廣告的右上角通常會設計有一個「？」的圖示，向使用者解釋為何會看到這則廣告，並另提供連結，看似可讓使用者設定日後拒絕再看到同樣的廣告。然而，當使用者點擊該連結後，卻被導向說明使用者的同意是如何被建立與管理的網頁，而非直接明瞭地關閉廣告選項，並伴隨著更多可能讓使用者更加困惑的解釋¹⁹。此種設計方式與使用者所預期得到的結果有所落差，將令使用者無所適從，構成「阻礙」的黑暗模式，並可能導致使用者放棄關閉廣告²⁰。

四、在社群媒體上行使個人資料相關權利

某些資料控制者可能以含糊不清的用語，透過「隱瞞」的黑暗模式帶過使用者得行使之權利，例如僅提及「某些」國家的監管當局會與資料控制者合作處理相關的投訴，而非清楚明確地告訴使用者，在歐盟的使用者有權向監管當局進行投訴²¹。

五、刪除社群媒體帳戶

有時當使用者欲刪除其社群媒體帳戶時，資料控制者並未清楚告知在帳戶被刪除後，使用者的資料是否會被一併刪除，也未在刪除過程中告知使用者，其「部分」資料在帳戶刪除後仍會被資料控制者所保留，使用者必須自行查找相關資訊，因而可能構成「隱瞞」之黑暗模式²²。

由上述從五個社群媒體使用者帳戶的生命週期階段中之舉例可知，許多常見的黑暗模式之設計實際上並不符合 GDPR 透明化之要件，即資料控制者必須以「簡潔、透明、可理解和易於近用的形式，並使用清楚易懂的語言」向資料主體提供資訊。特別是該些資料控制者試圖以模糊不清、易造成使用者混亂之用語或甚至未主動提供資訊之方式，使資料主體僅得知片面的資訊，進而做出可能不利於己的選擇。

肆、未來的影響

此指引草案的內容顯示歐盟針對資料保護更廣泛介入的趨勢。監管機構及法院正在追究提供網站、平台或其他消費者介面之公司的責任，蓋此些行為可能構成詐欺、操控或不正當地影響消費者，導致其行使隱私保護的選擇變少。

¹⁹ *Id.* para. 96.

²⁰ *Id.* para. 97.

²¹ *Id.* para. 139.

²² *Id.* para. 164.

此外，本指引對於非從事社群媒體業務的公司而言，仍有其指導意義，因此該等公司如欲避免其於社群媒體平台所從事的商業行為引發歐盟隱私機構的審視，則應參酌此指引作為其行為之準則。

