初探 GDPR 兒童同意權規範之遵循問題——

以網路服務產業為例

張安潔 劉瑋佳

摘要

歐盟「一般資料保護規則」於今（2018）年 5 月 25 日正式施行，凡涉及蒐集、使用歐盟公民之個人資料者都將受到規範。公司企業因此面臨是否確實遵循規範的挑戰，在網路服務產業又更是首當其衝，因為使用者可能是歐盟公民。GDPR 針對不同性質的資料有不同規範，其中對於蒐集使用兒童個資有特別嚴格的規範，鑑於兒童為許多網路服務平台大宗的使用者，如何取得有效同意，以合理蒐集及使用資料主體之個資便成為一大挑戰。因此，本文將探討歐盟就兒童同意與資料蒐集使用之規範內容，及網路服務平台產業面臨何種法令遵循之挑戰。此外，本文將整理歸納國外相關產業平台為遵循此規範之實踐方法，嘗試分析其優劣，可供台灣產業之借鏡參考。

1995 年歐洲共同體（European Community）通過了「個人資料保護指令（Data Protection Directive）」，以平衡歐盟成員國之間的個人資料保護水準，促進歐盟內部跨國間的資料流通[1]。雖然個人資料保護指令之宗旨與原則仍屬健全，惟其已無法避免歐盟內資料保護之規範斷層、法的不確定性或普遍大眾欠缺對於自然人之保護具有顯著風險之意識，特別是涉及網路活動時，各歐盟成員國對於當事人的權利與自由在保護程度上，存有不小的差異[2]。在歐盟各成員國處理個人資料方面，若保護權利的層次上存在落差，則可能會阻礙個人資料在歐盟內之自由流通，上述差異亦可能阻礙歐盟境內之經濟活動、造成不當競爭與妨礙機關履行其在歐盟法下的職責，而會有保護程度上之差異[3]。由於個人資料保護指令在執行及實務應用上之良莠不齊，為提升對歐盟公民之資料保護水準，歐盟於 2016 年通過「一般資料保護規則（General Data Protection Regulation, GDPR）」，並於今

[1] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, 50 [hereinafter Directive 95/46/EC].

[2] 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. 9, 2016 O.J. (L 119) 1, 38 [hereinafter GDPR].

[3] *Id.*

（2018）年 5 月 25 日正式施行，取代原先的個人資料保護指令。

在數位貿易頻繁的時代下，因為網路無遠弗屆的特性，可以觸及到世界各地的使用者，包括來自歐盟境內的使用者，因此企業更需要調整其網路平台的設計及隱私權保護政策，使其能符合 GDPR 的規範。在 GDPR 的規範中，資料控管者需徵得資料主體的同意，方得蒐集與使用其個資，而對於兒童的同意規範的要求又更加嚴格，意即該同意必須為兒童在知情下自主且明確地表示之同意，又若兒童不符最低年齡限制，則應取得父母之授權或同意，而以何種途徑取得父母同意以及驗證其為父母之身分，也將是一大挑戰。本文將介紹 GDPR 中對於兒童同意的規範，探究企業在實際遵循時可能會遇到的問題，並且借鏡國外相關的網路服務業者遵循之道，歸納整理各企業遵循方法的利弊。

壹、歐盟 GDPR 對於取得兒童同意的規範內容

在 GDPR 中規範關於同意之內容，要求企業所取得之同意須是資料主體基於其意思，透過聲明或明確肯定之行動，所為之自主（freely given）、具體（specific）、知情（informed）及明確表示之同意（unambiguous indication of the data subject's wishes）[4]。此外 GDPR 在第 8 條中亦對於取得兒童之同意有特別的規範，除了條文本身外，歐盟資料保護工作小組（Article 29 Data Protection Working Party, 以下簡稱工作小組）亦有進一步對於同意規範進行解釋[5]。本段將先介紹同意規範的內容，再進一步介紹兒童同意規範的要件與內容。

一、同意權規範的內容

GDPR 的核心目標是加強和協調個人資料保護，其規範不僅包含企業應如何處理、儲存和保護識別性個人資料之新規定，更包含罰款之懲罰性規定，以確保企業遵循 GDPR 之規範[6]。如若未遵循 GDPR 之規範，將可能面臨高達 2000 萬歐元的罰款，或如為企業者，其可能面臨最高達前一會計年度全球年度營業額 4% 之罰款，並以較高者為準[7]。根據 GDPR 第 4 條第 11 項之規定，所謂資料主體之「同意」，係指資料主體基於其意思，透過聲明或明確肯定之行為，所為自主性

[4] *Id.* art. 4(11).
[5] Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679, Adopted on 28 November 2017, as Last Revised and Adopted on 10 April 2018, WP259 rev. 01 [hereinafter Working Party Guidelines].
[6] Jesper Zerlang, *GDPR: A Milestone in Convergence for Cybersecurity and Compliance*, 2017(6) NETWORK SECURITY 8, 8 (2017).
[7] GDPR, art. 83.

具體、知情及明確之表示同意處理與其有關之個人資料[8]。以下將就同意的定義分述之。

（一）自主地表示同意

自主性意味著對資料主體的真正選擇和控制[9]。作為一般規則，GDPR 規定資料主體在沒有真正的選擇權、被迫同意，或如果不同意將會承受負面後果的情況下，所作成之同意無效[10]。如果該同意中含有不可商議之條件與條款的部分，則推定資料主體並非為自主地表示同意[11]。因此，如果資料主體無法在被侵害的情況下拒絕或撤回其同意，則該同意並非自主同意，由此可知，GDPR 將資料控管者與資料主體之間是否處於對等的平衡關係納入考量[12]。此外，評估是否自主地給予同意時，還應考慮將同意納入契約中，或提供 GDPR 第 7 條第 4 項之規定中所述服務的具體情況[13]。故一般而言，任何對資料主體施加不當壓力或影響的因素，阻止資料主體行使其自由意志，該同意應皆視為無效[14]。

（二）具體的同意

GDPR 第 6 條第 1 項第 a 款[15]確認資料主體的同意必須是針對一個或多個特定（specific）目的處理其個人資料，使資料主體可以對每個目的進行選擇，並確保資料處理的透明度[16]。GDPR 沒有改變這一要求，並且與知情同意的要求密切相關[17]。同時，必須按照詳盡（granularity）的要求來解釋，以獲得自主地同意[18]。為了符合「特定」這項要件，資料控管者必須[19]：具體化說明其使用目的，以避免挪用作其他目的之使用（purpose specification as a safeguard against function creep）、同意請求詳盡化，以及明確化獲得資料處理同意之相關資訊。

（三）知情同意

GDPR 強調同意必須係在資料主體已經知情的前提下取得[20]。為使資料主體

[8] *Id.* art. 4(11).
[9] Working Party Guidelines, at 5.
[10] *Id.*
[11] *Id.*
[12] *Id.*; GDPR, art. 7(4).
[13] Working Party Guidelines, at 5; GDPR, art. 7(4).
[14] Working Party Guidelines, at 5; GDPR, art. 7(4).
[15] GDPR, art. 6(1)(a).
[16] Working Party Guidelines, at 11.
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.* at 12.

在知情同意下作決定，以及理解其同意之內容，例如行使撤回的權利，資料控管者於獲得同意前提供相關資訊是非常重要的[21]。倘若資料控管者未提供相關資訊，猶如虛應故事一般地設置同意機制，而導致使用者同意之操作並非實際的同意，其個資處理之同意也將是無效的[22]。

（四）明確表示同意

GDPR 清楚地要求同意需要資料主體的陳述或明確的肯定行為，這意味著資料主體的同意必須以積極的行為或意思表示為之，且必須明顯同意具體特定的資料處理[23]。在個人資料保護指令第 2 條第 h 項中規定，同意係指資料主體表示其同意處理與其有關的個人資料的意願，而 GDPR 第 4 條第 11 項條以此定義為基礎，規定有效同意需要通過意思表示或明確的肯定行為[24]。

明確的肯定行為（clear affirmative act）意味著資料主體必須慎重地同意特定資料處理[25]。同意可以通過書面或記錄的口頭陳述蒐集，包括透過電子的方式，在不違反各國既存之契約法下，可以透過記錄的口頭陳述行使同意，但在徵得同意前必須注意資料主體可獲得之資訊，因為預設已勾選之選項框在 GDPR 規範下是無效的[26]。而資料主體之默示與不作為，即僅持續使用該服務，皆不視為主動之意思表示[27]。

資料控管者尚須注意，不能將「同意契約」和「接受所有一般條款和條件」一併視為獲得資料主體之同意，因為一般條款和條件的概括承諾不能被視為同意使用個人資料的明確肯定行為[28]。GDPR 不允許資料控管者提供已預設勾選之選項框或選擇退出之機制，這些選項框需要資料主體的干預才能防止達成協議，例如選擇退出鍵[29]。如資料主體之同意係基於電子方式之請求者，該請求必須清楚、簡潔，且不應對服務之使用造成不必要的中斷，資料主體必須以積極的作為表示同意[30]。在 GDPR 合理範圍內，資料控管者可以自由地制定符合其企業的同意流程，在這樣的情況下，資料主體之實際操作即視為明確的肯定行為[31]。

---

21 *Id.* at 13.
22 *Id.*
23 *Id.* at 15.
24 Working Party Guidelines, at 15; GDPR, art. 4(11); Directive 95/46/EC, art. 2(h).
25 Working Party Guidelines, at 16.
26 *Id.*
27 *Id.*
28 *Id.*
29 *Id.*
30 *Id.*
31 *Id.* at 17.

資料控管者應設計得以讓資料主體清楚明瞭的同意機制，確保資料主體明白資料使用之目的，必須避免含糊不清，意即確保同意內容之下的使用行為，和其他非同意內容之下的使用行為有所區隔[32]。因此僅僅持續使用網站並不是一種明確的肯定行為，因為該行為無從推斷資料主體對處理操作之明確意思表示[33]。

二、兒童同意權規範

在資料處理方面，與歐盟原本的個人資料保護指令相比，對於較弱勢之自然人，特別是兒童，GDPR 創建了一個額外保護層[34]。GDPR 第 8 條納入了額外的義務，以確保提高兒童在資訊社會服務方面的資料保護水準[35]。GDPR 增強保護兒童的原因在於，兒童可能不太了解相關的風險、後果和保護措施及使用者處理個人資料有關的權利[36]。根據 GDPR 第 38 號釋義指出，此特殊保護應特別適用於兒童個人資料的使用，以用於行銷或建立用戶檔案等特定目的，以及在使用直接向兒童提供的服務時，蒐集相關兒童個人資料之情況[37]。

根據 GDPR 第 8 條第 1 項規定，在適用同意的情況下，對於直接向兒童提供資訊社會服務，如果兒童年滿 16 歲，則兒童的個人資料處理應屬合法；如該兒童未滿 16 歲，僅限於其法定代理人授權或同意之範圍內，該等處理始為合法[38]。而關於有效同意的年齡限制，於 GDPR 第 8 條第 2 項中則規定，歐盟成員國可以透過法律為該等目的規定較低年齡，但不能低於 13 歲[39]。

為了獲得兒童的「知情同意」，資料控管者必須用淺顯易懂的字句，以向兒童解釋其將如何處理蒐集的資料[40]。倘若欲使其父母（以下概稱父母）之同意，那麼必須提供完整的資訊，以使父母做出明智的決定[41]。從上述內容可以清楚地看出，GDPR 第 8 條僅在滿足直接向兒童提供資訊社會服務之處理，或是基於同意之處理的情況下，而非所有資訊社會服務皆有適用[42]。以下將簡介兒童同意權之要件，包含資訊社會服務之定義、服務需直接向兒童提供、年齡之規範以及兒童的同意與親權責任之關係。

---

32 *Id.*
33 *Id.*
34 *Id.* at 23.
35 *Id.*; GDPR, art. 8.
36 Working Party Guidelines, at 23.
37 *Id.*; GDPR, recitals 38,.
38 Working Party Guidelines, at 23.; GDPR, art. 8(1).
39 Working Party Guidelines, at 23; GDPR, art. 8(2).
40 Working Party Guidelines, at 23; GDPR, art. 8(2).
41 Working Party Guidelines, at 23; GDPR, art. 8(2).
42 Working Party Guidelines, at 23; GDPR, art. 8(2).

（一）資訊社會服務

工作小組在評估 GDPR 中「資訊社會服務」之定義範圍時，援引了歐洲法院（European Court of Justice）過往的判例[43]。歐洲法院認為，資訊社會服務涵蓋線上締結或傳輸的契約和其他服務，如果該服務涉及兩個獨立之經濟活動，只要一方是在網路上提供的服務，例如在簽訂契約或與產品或服務相關的資訊，包括行銷活動中的要約和承諾，則該部份即被定義為資訊社會服務，而另一部份若是貨物的實際交付或分配，則不落入資訊社會服務的範疇[44]。故提供網路服務將屬於 GDPR 第 8 條規定中「資訊社會服務」的範圍[45]。

（二）直接向兒童提供服務

GDPR 第 8 條僅適用於直接向兒童提供的資訊社會服務，而非所有資訊社會服務[46]。如果資訊社會服務之提供業者明確表示，其僅向 18 歲或以上的潛在使用者提供服務，且網站內容或企業之行銷策略皆表明如此的意圖，則該服務將不被視為直接向兒童提供，因而不適用 GDPR 第 8 條規範[47]。

（三）年齡

GDPR 明確規定「歐盟成員國得訂定較低的法定年齡，惟年齡限制門檻不得低於 13 歲」，且資料控管者必須注意各歐盟成員國不同的法律規定，並同時考慮其服務的對象[48]。特別應注意的是，提供跨境服務的資料控管者不單要考慮其營業處所在地成員國的法律，更需要遵守資訊社會服務對象所在之歐盟成員國法律[49]。這取決於歐盟成員國選擇使用資料控管者營業處所在地，或資料主體處所作為其法律準據，且歐盟成員國在做出選擇時應以兒童最大利益作為首要考量，而工作小組亦鼓勵歐盟成員國在此問題上尋求一致的方案[50]。基於同意向兒童提供資訊社會服務時，資料控管者將需要做出合理的努力來驗證使用者是否已超過同意的年齡，且這些措施應與處理資料的性質和風險成比例[51]。

如果使用者聲明其已超過同意年齡，則資料控管者可以執行適當的檢查以

[43] *See* Case C-108/09, Ker-Optika bt v. ÀNTSZ Dél-dunántúli Regionális Intézete, 2010 E.C.J. I-12213, ¶¶ 22, 28.
[44] *Id.*
[45] Working Party Guidelines, at 24.
[46] *Id.* at 25.
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] *Id.*

驗證此陳述是否為真[52]。雖然在 GDPR 中對於「需要採取合理的努力來驗證年齡」之要求並不明確，但是如果兒童在未達有效同意年齡的情況下同意該資訊社會服務，則使用者所為之同意是無效的，如此一來致使企業對該資料之處理變成非法[53]；而當使用者聲明其低於同意年齡，則資料控管者可以接受此聲明而無需進行檢查，但仍需進一步獲得父母行使授權同意並驗證之[54]。

（四）兒童的同意和親權責任

關於父母的授權，GDPR 沒有規定取得父母同意或確定某人有權執行此行動的實際運作方法[55]。工作小組建議在兒童之法定代理人授權或同意之情況，資料控管者應作出合理努力，在考量現有科技之情況下，確認該法定代理人之同意或授權，且須同時兼顧資料蒐集最小化的原則，亦即以適當、相關且限於處理目的所必要，其著重在獲取有限的資料，例如蒐集父母的聯繫方式即可[56]。

在驗證使用者年齡足以行使的同意，以及在驗證代表兒童同意的人是父母方面，驗證方式之合理性可能取決於處理以及可用的技術[57]。在低風險案例中，透過電子郵件驗證行使親權者之身分可能即已足夠；反之在高風險情況下，可能需要提供更多證據，以便資料控管者能夠根據 GDPR 第 7 條第 1 項驗證和保留資訊，而可信第三方提供的驗證服務，可以協助資料控管者處理最小化之個人資料量[58]。工作小組承認驗證可能存在著挑戰性，例如兒童在尚未建立身份足跡的情況下行使同意，或者在驗證親權的行使上有困難[59]。在決定採取何等措施始為合理時，應將上述情況也納入考量，且資料控管者也要不斷審查其處理流程和可用技術[60]。

資料主體擁有完全控制處理其個人資料之權利，親權行使者雖能同意兒童個人資料之處理，但當兒童達到同意年齡，則得以修改或撤銷同意[61]。在實務中，這代表著如果兒童尚未為任何同意行為，若親權行使者或被授權代為行使親權者，直接同意兒童資料之處理，則該同意將視為有效同意[62]。根據 GDPR 第 7 條

52 *Id.*
53 *Id.*
54 *Id.*
55 *Id.* at 26.
56 GDPR, arts. 8(2), 5(1)(c).
57 Working Party Guidelines, at 26.
58 *Id.*
59 *Id.* at 27.
60 *Id.*
61 *Id.*
62 *Id.*

第 3 項規定，在達到同意年齡後，兒童將得自行撤回同意，GDPR 中亦規範兒童在使用一些特定服務時不需要父母的同意，例如直接向兒童提供的預防或諮詢服務，或是透過線上聊天服務向兒童提供保護服務等[63]。

貳、網路服務產業中兒童同意規範的遵循問題

網路上許多服務需要靠個人資料才能運行，因此資料主體每天都會收到多個同意請求，而這些請求則需要透過點擊和滑動來獲得答案[64]。當遇到太多次同意要求時，可能導致一定程度的點擊疲勞，同意機制的實際警告效果就會減弱，可能會發生同意問題不再被閱讀的情況[65]。這對資料主體來說是一種特殊風險，因為原則上同意請求未經資料主體同意的情況下為非法的行為，故 GDPR 要求資料控管者制定解決此問題之方法[66]。以下將就網路服務產業與兒童同意規範相關之原因與遵循上可能會遇到的問題作一分析。

一、網路服務產業與兒童同意規範相關之原因

社交平台（Social Network Sites）為網絡服務之一環，具有三個特點，分別為[67]：允許個人在網路上建立公共或半公開的個人資料、清楚表述與使用者共享交流之其他使用者列表，以及查看並瀏覽使用者與其他使用者的聯繫列表[68]。社交平台的會員創建個人簡歷，包含使用者的個人資料，例如使用者的姓名、年齡、性別、地點和婚姻狀況，以及圖片和其他詳細資訊。如此一來，使用者可以與朋友進行溝通，且可以選擇與其感興趣的陌生人聯繫，成為具有共同興趣之網路社群一員[69]。

隨著科技不斷進步，兒童越來越早接觸網路世界，透過社交平台維持友誼與建立人際關係習以為常，以達到網路結識朋友的目的[70]。儘管有特地為兒童創設之社交平台，但兒童已經越趨活躍於為成人所創設之社交平台，如 Facebook、Instagram、Twitter 和 Snapchat 等等。兒童鮮少意識到社交平台蒐集的個人資料，包括姓名、出生日期、關係狀態、興趣和照片，皆明確地（例如性別）或隱含地

63 *Id.*; GDPR, art. 7(3).
64 Working Party Guidelines, at 17.
65 *Id.*
66 *Id.*
67 Danah Boyd & Nicole Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13(1) JOURNAL OF COMPUTER-MEDIATED COMMUNICATION, 211(2007).
68 *Id.*
69 BRÄUTIGAM, TOBIAS JA MIETTINEN & SAMULI (TOIM.), DATA PROTECTION, PRIVACY AND EUROPEAN REGULATION IN THE DIGITAL AGE 112 (2016).
70 *Id.*

（例如性取向或宗教信仰)揭示個人訊息，所以社交平台在處理該等個人資料時，必須得到資料主體自主地表達其知情同意始屬合法[71]。

二、遵循上可能會遇到的問題

前述平台蒐集使用個人資料皆必須取得資料主體的同意，而取得有效之兒童同意尚需檢視該兒童行使同意時是否符合年齡規定，並且該同意是否為明確的知情同意。基於前述要件，取得兒童同意權將可能遇到以下問題：

（一）年齡驗證需考量各國分歧的法規

雖然社交平台規定禁止兒童使用者成為該會員，然而社交平台通常不會要求使用者提供其年齡、身份驗證或父母同意作為註冊帳戶時的先決條件[72]。反之，社交平台多仰賴使用者自我認證（self-certification）的方式，以證明該使用者超過所允許的年齡[73]。自我認證的方式諸如勾選方框、輸入出生日期或是拒絕兒童進入的視窗[74]。更甚者，有些網站從未要求使用者確認出生日期，僅依據社交平台的條款聲明如「您必須年滿 13 歲才能使用本服務」，來認證使用者年齡[75]。

為避免遇到處理兒童個人資料須先取得其明確同意之困難，社交平台資料控管者透過設定該平台會員之最低年齡限制，以禁止不符最低年齡限制的兒童使用該平台[76]。由於社交平台之使用者來自於世界各國，而各國對最低年齡之限制不盡相同，因此平台設計遵循方法時須同時考量各國的相關規範[77]。

（二）用語晦澀難使兒童知情同意

為使兒童明確同意社交平台對其個人資料數據的處理，兒童必須具備理解該社交平台上服務條款與隱私聲明的能力[78]。由於大多數的社交平台最初是為成年人而設立，其條款和責任聲明的用語通常對兒童而言過於艱澀複雜，因此兒童自然會轉向父母尋求解釋與協助[79]。然而有學者在社交平台隱私政策的分析中發

[71] *Id*. at 115.
[72] *Id*. at 116.
[73] *Id*.
[74] *Id*.
[75] *Id*.
[76] *Id*.
[77] *Id*.
[78] *Id*. at 115.
[79] *Id*.

現，各社交平台的隱私政策長短不一，且其內容用語幾乎為隱晦的法律術語，即使是一般成年使用者也難以理解[80]。

（三）實務操作之綜合問題

工作小組以線上遊戲平台為例，提供資料控管者遵循之參考[81]。基於希望確保兒童客戶僅在其父母的同意下訂閱其服務，因此資料控管者應依循以下四步驟[82]：如若使用者需表示其未達到同意年齡時，則需要求使用者說明其年齡是否小於或超過 16 歲，或各國法定同意年齡；向兒童提供服務之前，該平台需先通知兒童的父母，以徵得其同意或授權處理，因此使用者需要提供父母的電子郵件；該平台透過電子郵件聯繫兒童的父母，以獲得其同意，並採取合理的步驟確認其為行使親權之人[83]。

參、遵循兒童同意規範之實務實踐

GDPR 在兒童之數據蒐集及使用的同意規範上要求嚴格，加上舉凡可能觸及歐盟公民的企業都需要遵循 GDPR 之義務，所以企業會在遵循上仍會遇到許多問題。台灣的網路服務產業亦會面臨到相同的問題，該如何遵循相關規定乃是一重要的課題，而探究國外企業已先行做的遵循因應方法，可以作為遵循方法上之參考。網路平台之遵循手法可從其隱私權政策條款，以及使用者登入註冊之方式觀之，故本段將針對國外相關網路服務平台之隱私權政策中就兒童同意之規範，與實際登入註冊之方式進行整理，歸納出不同形式的遵循方法或策略，並分析其利弊[84]。

一、直接排除兒童使用

有些服務平台會直接限制對於低於規定年齡之使用者使用平台服務，Facebook、Twitter、Snapchat 等社交平台多採取此種方式[85]。以 Facebook 為例，

[80] *Id.*
[81] Working Party Guidelines, at 26.
[82] *Id.*
[83] *Id.*
[84] 本段所整理歸納之網路服務平台隱私政策包含：Funbrain、Brianpop、Startfall、Funology 等教育網站。FUNBRAIN, https://www.funbrain.com/privacy-policy (last visited Dec. 10, 2018); STARFALL, http://www.starfall.com/ (last visited Dec. 10, 2018); BRAINPOP, https://www.brainpop.com/about/privacy_policy/ (last visited Dec. 10, 2018); FUNOLOGY, https://www.funology.com/privacy-policy/ (last visited Dec. 10, 2018).
[85] FACEBOOK, https://www.facebook.com/help/157793540954833 (last visited Dec. 10, 2018); TWITTER, https://twitter.com/en/tos (last visited Dec. 10, 2018); SNAPCHAT, https://www.snap.com/en-US/privacy/privacy-policy/ (last visited Dec. 10, 2018).

Facebook 直接限制低於 13 歲的兒童不得註冊及使用平台服務，並且設有檢舉機制，倘若其他使用者或兒童之父母發現有未滿使用 13 歲之兒童謊報年齡使用 Facebook 之情況，可以向 Facebook 檢舉[86]。

此種直接排除兒童使用之遵循方法的優點在於，從企業的角度而言就可減少驗證父母同意的法律遵循成本，也可以降低違法蒐集或處理兒童的資料的風險；對使用者而言也可以保障兒童的隱私權，避免兒童的個人資料暴露於網路上，或被違法的蒐集使用。惟此種遵循方法亦有潛在缺點存在，如果服務平台完全杜絕兒童的使用，在廣告的投放上將會遇到限制，例如跟兒童相關的產品或服務廣告就無法觸及到最直接的目標客群，這也可能成為企業的另一種商業成本或利益上的損失。

二、取得父母同意

大部分社交平台及部分教育平台都需要藉由蒐集使用者個人識別資訊運作，因此在使用特定服務平台時，若兒童需要註冊成為會員，便可能會蒐集到個人識別資訊，如此將涉及到資料主體行使同意權與否的情形。在兒童同意權需要取得父母同意的規定下，如何驗證得到父母之同意，歸納出的類型有直接與間接兩種同意，以下分述之。

（一）要求父母直接同意之方式

在徵得父母同意方面，實務上有平台採取的方式是，直接要求父母同意。若使用者低於 16 歲或為該平台規定的年齡限制以下者，該平台業者會要求父母或監護人用電子郵件或簡訊方式，對兒童使用者之使用表示同意，例如美國教育平台 Funbrain[87]。採用此種遵循方式的企業，應考量兩個可能面臨之問題：其一是倘若使用者謊報年齡，可能造成企業違法蒐集使用該使用者資料的風險；另一方面若要確實要求兒童的父母落實驗證門檻，可能會成為一個使用者使用平台服務的障礙，亦有可能增加企業的遵循成本，因此實務上確實也有些平台並沒有真的強迫使用者交付父母同意證明。

採取此種遵循方法的優點在於，因為針對兒童特定的資料處理或蒐集確實有得到兒童父母的同意，企業可以確保其在蒐集或處理兒童的資料時是合法的，可以避免在法律遵循上的不確定性；惟採取此種遵循方法的缺點在於，誠如前段有

[86] *See* Facebook, https://www.facebook.com/help/157793540954833 (last visited Dec. 10, 2018).
[87] *See* FUNBRAIN, https://www.funbrain.com/privacy-policy (last visited Dec. 10, 2018).

提及的遵循成本問題，若企業要確實落實取得父母之同意證明，不論是用簡訊或電子郵件的形式皆會增加程序的繁雜程度，進而可能提高人事與法遵的成本。

（二）視為父母間接同意之方式

除了直接要求父母回傳同意書之方式之外，有些較具規模的教學平台會要求註冊並付費才能使用，而支付方式便需要提供信用卡號，此可當作一種間接認定父母同意的方法，例如 Brianpop 與 Startfall 等美國兒童學習教育平台[88]。除此之外，有些教育平台必須藉由學校機構名義註冊，例如要求只能使用 G Suite 教育版的 Gmail 註冊[89]。在前述提及之 Brianpop，亦有這種透過學校機構把關的註冊方式，也可被認為是一種間接認定父母同意的方法[90]。

通常採取這種遵循方法的平台，主要適合需付費的平台或與學校有產學合作者。此遵循方法之優點在於，相對於要取得父母直接的同意證明會需要較多的程序跟成本，企業可以透過這種類似間接取得父母同意的方式降低法遵成本；惟其亦有潛在的缺點，GDPR 要求資料控管者要徵得資料主體的同意必須是直接明確的同意，因此這種類似間接同意的方式是否可被認為屬於明確的同意，存有模糊地帶，可能會有違法的風險。

三、避免蒐集兒童個人識別資料

有些服務平台會為了避免需要進一步徵得父母之同意證明，會採取直接不蒐集使用者個人識別資訊的策略。此類平台都會在隱私政策中強調不蒐集個人識別資訊，僅蒐集匿名資訊。使用者在平台使用服務時，不需要輸入姓名，若需要輸入姓名，也強調該姓名只會顯示於使用者電腦，不會傳輸回公司例如 Brianpop、Funbrain 與 Funology 等美國知名教育學習平台[91]。採此方法的教育平台，在使用操作上多不需要進行註冊即可使用，故業者也可避免蒐集到使用者個人識別資訊。

採取這種遵循方法的優點在於，若企業可以透過技術在完全避免蒐集兒童的個人識別資訊下運作，則可以避免進入徵得父母同意較困難的步驟；惟使用這種方法的缺點在於有兩的方面需要考量。一來業者需要具備相關的技術，從平台設

88 *See* STARFALL, http://www.starfall.com/ (last visited Dec. 10, 2018).
89 G Suite 教育版：Google 為學校推出 G Suite 教育版，是一套整合式通訊及協作解決方案，可為學校代管電子郵件、日曆和即時通訊服務。GOOGLE, https://support.google.com/a/answer/139019?hl=zh-Hant (last visited Dec. 10, 2018).
90 *See* BRAINPOP, https://www.brainpop.com/about/privacy_policy/ (last visited Dec. 10, 2018).
91 *See* FUNOLOGY, https://www.funology.com/privacy-policy/ (last visited Dec. 10, 2018).

計的層面避免蒐集到使用者個人識別的資訊，相關技術可能會是成本考量之一。二來從網路服務業者的營運角度而言，使用者的個人識別資訊是重要的資源可以幫助業者了解使用者習慣，進而調整行銷策略或更新服務，若業者完全不蒐集該等資訊，亦有損失資源上的疑慮，值得深思。

肆、結論

GDPR 不僅提高歐盟公民的資料保護之水準，對兒童使用網路服務更是增添保障，但同時也帶給歐盟外的企業在法律遵循上的挑戰。資料控管者要蒐集使用個資，必須是在資料主體知情同意之情況下，亦須檢視各國年齡限制，又若兒童為符合最低年齡限制，則需透過父母之授權同意。現今兒童日漸活躍於網路上，企業如何權衡商業貿易利益，以及落實遵循 GDPR 對兒童資料的保護是一重要的課題。從了解規範直到落實遵循之間，往往還有一段距離及困難有待探究。借鏡國外產業的遵循方法，雖各有其利弊，但仍值得作為我國未來關於兒童資料保護發展方向的參考。