簡介英國新資料保護法草案

江庭瑀 編譯

摘要

英國政府於今（2017）年 9 月 14 日公告「新資料保護法草案（Data Protection Bill）」，草案援引歐盟「資料保護的一般規則（General Data Protection Regulation）」與「法律執行指令（Law Enforcement Directive）」之內容，期望制訂更完善的個人資料保護規範以取代 1998 年的舊法。草案分為 5 個主要部分：一般資料處理、執法相關資料處理、國家安全資料處理、資訊委員會（Information Commissioner's Office）之地位與功能和執行與罰則。英國政府對本次新法抱持高度的信心與正面期待，然外界多批評法條內容過於繁雜與破碎化，可能導致法條適用的結果與立法目的背道而馳，不但僅能賦予人民有限的資料保護權利，亦可能成為其與歐盟國家資料傳輸間的隔閡。

「1998 年資料保護法（Data Protection Act 1998, DPA）」為英國目前的資料保護法律，然因其與歐盟「資料保護的一般規則（General Data Protection Regulation, GDPR）」存在太多規範差異，為避免民眾與國內企業產生混淆，英國政府決定制訂新法。「新資料保護法草案（Data Protection Bill，下稱草案）」除增訂符合數位時代科技潮流的規範外，亦借鑑歐盟法納入許多促進跨國資料傳輸的條文。本文第壹部分將敘述草案的立法背景與目的，英國政府在對外聲明的文件中，將草案分為五個部分，該內容於第貳部分分別介紹之，第參部分蒐集各界對草案的評析與意見，藉以瞭解本草案可能的缺失，最後作一結論。

壹、立法背景與目的

英國預計在 2019 年春天脫離歐盟，因此，於 2018 年 5 月 25 日生效的 GDPR，將會在英國脫歐前直接適用於英國。在英國脫歐後，依據「歐盟（退出）草案（European Union (Withdrawal) Bill）」第 3 條[1]，GDPR 條文將成為內國法，繼續適用於英國。為使該法規在國內順利運作，英國必須在 GDPR 賦予會員國的裁量權限內，填補其與現行

[1] European Union (Withdrawal) Bill, art. 3(1), (providing that: "Direct EU legislation, so far as operative immediately before exit day, forms part of domestic law on and after exit day.").

國內法之落差。再者，由於 GDPR 僅適用於歐盟管轄權範圍內之「個人資料處理」，會員必須檢視其國內相關立法是否也適用於此部分的個人資料處理事項[2]。

DPA 塑造了當今英國資料保護的法律架構，然而該法施行至今已逾 20 年，許多條文需要更新，以順應數位時代資料產生與使用的模式。隨著企業與政府持有的個人資料量與日俱增，制定穩固的資料保護法律及適當防衛措施的需求漸高。除為達到上述目的，草案亦希望確保英國脫歐後，國內的刑事司法機構能繼續與其他歐盟國家共享資料，一同打擊犯罪並對付國安威脅[3]。

草案之目的為：替英國制定全面性且現代化的資料保護架構，並對不法行為實施更嚴厲的制裁；建立與 GDPR 一致的新標準以保護個人資料；賦予人民更多對於資料使用的控制權；並在保留 DPA 創設的「排除（derogations）[4]」與「豁免（exemptions）[5]」條款下，提供移轉或刪除資料的新興權利。除此之外，草案亦打算為英國執法機構及情報單位量身定做特殊架構，一方面保障受害者、目擊證人及嫌疑人的權利，另一方面亦確保國家能對付變化多端的全球威脅[6]。

草案甫進入國會議事程序。英國政府於今（2017）年 8 月宣布其欲倡議新資料保護法草案以解決上述問題，草案及詳盡的附註文件已於 9 月 13 日提交上議院[7]。

貳、英國新資料保護法草案介紹

「新資料保護法草案」在接近 200 頁的篇幅中包含 7 個章節，以整體架構而言，主要由 5 個部分構成，分別為：一般資料處理、執法相關資料處理、國家安全資料處理、資訊委員會之地位與功能和執行與罰則，本文將重點式介紹每部分之內容。

一、第一部分：一般資料處理

---

[2] Francis Aldhouse, *The UK Government Publishes the Data Protection Bill*, BIRD & BIRD LLP, Sept. 20, 2017, https://www.twobirds.com/en/news/articles/2017/uk/uk-government-publishes-data-protection-bill (last visited Nov. 9, 2017).

[3] HER MAJESTY'S GOVERNMENT, DATA PROTECTION BILL: SUMMARY ASSESSMENT 1, *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644636/2017-09-12_Data_Protection_Bill_IA_final.pdf (last visited Nov. 9, 2017).

[4] 在一般英美法的規定中，「derogation」指的是條文或契約條款的部分免除適用；然而在歐盟法上，derogation 亦可指歐盟會員國延後適用歐盟法規的部分要素，或是會員國基於本國情況而選擇不予適用特定條文。參照 GDPR 第 23 條意旨，此處的 derogation 應指會員國在符合相關要件時，得不適用 GDPR 對於該種個人資料保護所設的權利與義務內容；*See* Black's Law Dictionary (10th ed. 2014).

[5] 當豁免規定存在時，即便該行為違反一法律規定，行為人仍可豁免於義務與罰則；*See* Black's Law Dictionary (10th ed. 2014)。

[6] *Id.*

[7] Francis Aldhouse, *supra* note 2.

相關規範規定於草案本文的第 3 條至第 26 條，以及附件 1 至附件 6[8]。本部分規定將 GDPR 之資料處理原則適用於所有一般資料處理，並以英國為 GDPR 使用背景給予部分定義更明確的解釋[9]。

GDPR 生效後，歐盟會員國境內的個人資料處理行為必須完全符合該法規範[10]。由於 GDPR 較過往的「歐盟資料保護指令（EU Data Protection Directive）」保護密度為高，賦予資料主體更詳盡的權利種類，草案也將這些元素納入本次新法範圍，包括：

（一）個人資料

GDPR 第 4 條「個人資料的定義」大幅擴張個人資料的範圍，草案遵循改革潮流，將數個 DPA 中未涵蓋的資料種類納入個人資料保護範圍，例如：IP 位址、網路 Cookie，這些改變係為避免有心人利用網路瀏覽紀錄，以鎖定特定使用者[11]。

（二）隱私

由 GDPR 第 7 條「同意要件」發展而來。現今許多網站強迫拜訪者以「選擇退出（opt out）」之方式，拒絕網站蒐集其電子郵件或電話號碼，例如在網路表單的最下方，要求使用者勾選「拒絕網站利用其個資」；換句話說，在瀏覽者經常忽略隱私條款的情況下，其經常被推定同意該隱私條款。新法將要求此種同意必須明確，讓使用者以「選擇加入（opt in）」之方式同意行銷公司取得其個資，並能夠意識到自己的資料正被傳遞至行銷公司[12]。

（三）資料近用權

[8] Eduardo Ustaran & Sam Choi, *UK's Draft GDPR Implementation Law: The Starting Point*, HOGAN LOVELLS, Sept. 27, 2017, http://www.hldataprotection.com/2017/09/articles/international-eu-privacy/uks-draft-gdpr-implementation-law-the-starting-point/?utm_source=dlvr.it&utm_medium=twitter (last visited Nov. 9, 2017).
[9] William RM Long & Thomas Fearon, *UK Government Publishes Draft Data Protection Bill*, SIDLEY AUSTIN LLP, Sept. 15, 2017, http://datamatters.sidley.com/uk-government-publishes-draft-data-protection-bill/ (last visited Nov. 9, 2017).
[10] Detlev Gabel & Tim Hickman, *Chapter 7: Lawful Basis for Processing – Unlocking the EU General Data Protection Regulation*, WHITE & CASE LLP, July 22, 2017, https://www.whitecase.com/publications/article/chapter-7-lawful-basis-processing-unlocking-eu-general-data-protection (last visited Nov. 9, 2017).
[11] James Titcomb, *Data Protection Bill: How Will the New Laws Affect You?*, THE TELEGRAPH, Aug. 7, 2017, http://www.telegraph.co.uk/technology/0/data-protection-bill-will-new-laws-affect/ (last visited Nov. 9, 2017).
[12] *Id.*

此項權利源自 GDPR 第 15 條。資料主體將會取得更多有關其個人資料如何被處理的資訊，這些資訊必須以清楚、可明瞭的態樣呈現[13]。

（四）被遺忘權

此項權利源自 GDPR 第 17 條。當資料主體不再希望他們的個人資料被使用，且資料控管者（data controller）亦無合法依據保留該資料時，必須刪除資料[14]。在新法規定下，消費者將能夠要求企業或組織取用或刪除其個人資料，這將賦予資料主體對刪除資料的細節具有更多控制權。草案進一步擴張 GDPR 的規定，要求社群媒體公司在本人的請求下，必須刪除其在 18 歲以前的貼文（post）[15]。

（五）資料可攜權

此項權利源自 GDPR 第 20 條，其目的係在使資料主體更容易在服務提供者（service providers）間移轉個人資料。基於資料主體的請求，資料控管者必須：

1. 以結構化、普遍使用及可被機器讀取的格式，提供資料主體其當初提供給資料控管者之個人資料的副本（而非已經被資料控管者處理過的資料）；
2. 不阻止資料主體將其個人資料傳送給其他資料控管者；
3. 當技術允許時，資料主體有要求其個人資料在資料控管者間直接傳輸的權利[16]。

（六）自動化數據處理

此項權利源自 GDPR 第 22 條。當個人使用演算法將其資料予以歸類建檔（profiled）時，例如：有關個人之健康評估、財富管理或人身移動狀態等，資料主體將可要求視該等歸類建檔為人為施作而來[17]，如此一來資料主體將可妥善維護其權利。目前像保險、工作申請等範疇正日益依賴自動化系統進行歸類建檔，所以此類規定的重要性逐漸成長[18]。

[13] Tim Smith, *The Data Protection Bill: UK's Answer to the GDPR*, BLM, Oct. 30, 2017, https://www.blmlaw.com/news/the-data-protection-bill-uk-8217-s-answer-to-the-gdpr (last visited Nov. 9, 2017).
[14] *Id*.
[15] James Titcomb, *supra* note 11.
[16] Tim Smith, *supra* note 13.
[17] James Titcomb, *supra* note 11.
[18] *Id.*

草案的另一項功能是將 GDPR——或其他類似的規定——擴及其原先未適用的資料處理領域。舉例來說，GDPR 並不適用於法律執行和情報活動，但英國自願將與 GDPR 相像的規範適用於此些範疇，詳細內容可見草案的第三章與第四章[19]。

此外，草案在一般資料處理規範上，亦援引 GDPR 下的豁免及排除條款[20]，並於草案的附件 2 至附件 4 詳細列出豁免與排除的內容及範圍。在立法考量上，草案致力於保留現行國內企業已適用的豁免或排除條款，這代表新法可能不會刪除與金融服務、新聞業者、研究與法律機構等相關的豁免條款，此項措施顯然會受到許多組織的熱烈歡迎[21]。

二、第二部分：執法相關資料處理

相關規範規定於草案本文的第 27 條至第 79 條，以及附件 7 與 8[22]。本部分立基於 2016 年 4 月歐盟所通過的「法律執行指令（Law Enforcement Directive, LED）」。LED 以管控「警察及刑事司法機構為刑事犯罪所為之預防、調查、偵查或追訴，以及執行刑罰所為之個人資料處理行為與該種資料的自由流通」為宗旨，適用於與執法目的相關之跨境個人資料處理內容[23]。為確保法規的一致性，草案中的此部分規定亦適用於國內相同的資料處理行為，這種設計能夠確保執法相關資料處理制度，在英國國內與跨境間適用同一規範[24]。

三、第三部分：國家安全資料處理

相關規範規定於草案本文的第 80 條至第 111 條，以及附件 9 至 11[25]。國家安全條款並不在歐盟法的架構之下，因此 GDPR 與 LED 皆未制定以國家安全為目的的個人資料處理規定。同樣的，上述兩者亦未設計出適用於情報處理資料之目的之情況[26]。有鑑於此，草案創設出新架構，使情報單位的個人資料處理將由一套不同制度規範，該制度

---

[19] Robin Hopkins, *The Data Protection Bill: a brief overview*, THOMSON REUTERS PRACTICAL LAW, Sept. 25, 2017, https://uk.practicallaw.thomsonreuters.com/w-010-5346?transitionType=Default&contextData=(sc.Default) (last visited Nov. 9, 2017).

[20] Praveeta Thayalan, *A First Look at the New UK Data Protection Bill*, LEXOLOGY, Sept. 19, 2017, https://www.lexology.com/library/detail.aspx?g=c5925834-76e3-4b85-9b53-121e738e7a83 (last visited Nov. 9, 2017).

[21] Rocio de la Cruz, *Data Protection Bill: All you need to know*, TEISS, Sept. 15, 2017, https://teiss.co.uk/features/new-data-protection-bill-need-know/ (last visited Nov. 9, 2017).

[22] Eduardo Ustaran & Sam Choi, *supra* note 8.

[23] HER MAJESTY'S GOVERNMENT, DATA PROTECTION BILL FACTSHEET- LAW ENFORCEMENT DATA, *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644826/2017-09-13_Factsheet03_law_enforcement.pdf (last visited Nov. 9, 2017).

[24] *Id*.

[25] Eduardo Ustaran & Sam Choi, *supra* note 8.

[26] HER MAJESTY'S GOVERNMENT, DATA PROTECTION BILL FACTSHEET- NATIONAL SECURITY DATA PROCESSING, *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644829/2017-09-13_Factsheet04_national_security__1_.pdf (last visited Nov. 9, 2017).

將會依循更新後的歐洲理事會（Council of Europe）之「保護自動化處理個人資料公約（Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data）」中相關的國際標準進行管制[27]。

四、第四部分：資訊委員會之地位與功能

相關規範規定於草案本文的第 112 條至 136 條，以及附件 12 至 14[28]。草案中規範了資訊委員會（Information Commissioner's Office, ICO）之一般功能及義務，除依現有的 DPA 規定草擬資料分享準則，亦要求其編纂直接行銷準則並附上實務指引，內政部部長也可能額外要求 ICO 擬定其他業務指導性準則。這些準則必須送交給內政部部長，再由內政部部長送入國會，國會將有 40 天的期限回應準則，逾期將直接頒布。即便違反準則不能直接使行為人負法律責任，法院仍得於相關法律程序中將準則條文納入考量[29]。

草案亦賦予 ICO 發布評估通知的正式權力。在 DPA 的規定中，評估通知一般係針對政府機關發布，僅在特定情況下，主管機關得以命令授權 ICO 向特定公共機構或資料控管者發布評估通知。目前提出的草案似乎欲使 ICO 在受到部分限制下，對任何資料控管者或處理者（data processor）發布評估通知，此舉代表了 ICO 之權限從原先只能對資料控管者或處理者進行自願性稽核，首次提升為全面性稽核[30]。

五、第五部分：執行與罰則

相關規範規定於草案本文的第 112 條至第 136 條，以及附件 12 至 14[31]。草案允許 ICO 對資料控管者或處理者施以行政罰，最嚴重的違法行為可能被課處高達 1 千 8 百萬英鎊或 4%年度全球營業額的罰款，此額度反映了 GDPR 中罰款的最大限度[32]。再者，與 GDPR 的規定相異，草案授權 ICO 得提起刑事訴訟，例如：當資料控管者或處理者意圖更改紀錄，以規避他人依資料主體閱覽請求之資訊公開時，ICO 即得對其提出控訴[33]。

草案亦將部分有關個人資料處理之行為入罪化，以下將就最相關之罪行進行介紹：

---

[27] *Id.*
[28] Eduardo Ustaran & Sam Choi, *supra* note 8.
[29] Praveeta Thayalan, *supra* note 20.
[30] *Id.*
[31] Eduardo Ustaran & Sam Choi, *supra* note 8.
[32] William RM Long & Thomas Fearon, *supra* note 9.
[33] *Id.*

（一）故意妨礙或未協助（在無合理事由的情況下）資訊委員進行其權責範圍內的個人資料調查。

（二）未能遵守資訊通知，包括明知或輕率地做成不實的陳述以回應該通知。

（三）在未得資料控管者的同意下，明知或輕率地非法取得或揭露個人資訊。

（四）在未得資料控管者的同意下，明知或輕率地重新識別已去識別化之個人資料。

（五）為防止全部或部分資料公開，將原可經資料主體閱覽請求而獲得之資訊修改、損壞、封鎖、消除、銷毀或隱匿[34]。

參、外界評析

英國科技部長 Matt Hancock 表示草案將帶給英國國民世界上最健全又最有力的資料保護法，它將賦予民眾更多對於個人資料的主控權，並為英國脫歐做好準備。資訊委員 Elizabeth Denham 亦同意此番論述：「我們很高興見到政府認可了資料保護的重要性，在數位經濟世界中，強化資料保護將會帶給大眾福祉[35]。」

相對於政府官員的樂觀，有論者批評草案的架構與修法內容是「高度保守的」，認為政府尋求盡可能貼近現行法律內容。有鑑於 GDPR 的施行日期逐漸逼近、新法必須置入 LED 規範，再加上脫歐程序的進行，其實不難理解政府採行此立場的原因，更可基於上述原因，推斷出即便在立法程序中遭遇反對，政府仍會嚴守同樣的態度[36]。在此情況下，草案新增的權利符合數位時代下個人資料型態轉變的潮流，應予肯定，然因 GDPR 僅就這些權利設有初步性、通盤性的規範，英國新法內容又過於龐雜且涵蓋許多豁免規定，實際執行上是否真能保障個人資料權利，值得深入研究探討。

亦有論者認為草案的藍圖相當錯綜複雜，這項結果源自政府欲在單一法律中同時滿足數種目的[37]。英國國家資料保護及資訊自由協會（National Association of Data Protection and Freedom of Information Officers）主席 Jon Baines 形容草案為「一團混亂」，並說明

[34] Praveeta Thayalan, *supra* note 20.
[35] Barney Thompson, *UK data bill to bring more protection and bigger fines*, FINANCIAL TIMES, Aug. 6, 2017, https://www.ft.com/content/bbdbdb04-7935-11e7-90c0-90a9d1bc9691 (last visited Nov. 9, 2017).
[36] Francis Aldhouse, *supra* note 2.
[37] Andrew Dunlop, *UK government introduces Data Protection Bill to Parliament – what are the key changes?*, BURGES SALMON, Oct. 6, 2017, https://www.burges-salmon.com/news-and-insight/legal-updates/data-protection-bill/ (last visited Nov. 9, 2017).

這表示對英國而言，制定一個能在脫歐後與歐盟繼續貿易與合作的法案是十分困難的[38]。

舉例而言，由於草案第 31 條（7）項將歐盟國家視為一個整體，當英國脫歐後，英國本身將成為「第三國」，即「會員國以外的國家或地區」[39]。如同草案第 71 條（1）項所明文：「企業可能無法傳送資料至第三國[40]。」屆時如果沒有相關協議，將會對資料共享造成巨大的影響。在沒有資料協定的情況下，英國如要與其他歐盟國家分享資料，必須進行「適當性評估（adequacy assessment）」[41]，但一個適當性評估通常會花費超過一年的時間。除此之外，關於適當性評估的保證書（endorsement）將不會發送給歐盟國家，因為適當性評估預先排除了歐盟會員國參與的必要性。如果英國脫歐時雙方未做成任何協議，歐盟組織在與英國分享資訊時，必須以具有拘束力的契約代替，否則就得使用適當性評估的方式[42]。

最後，GDPR 雖明確地給予會員國之立法機構在數種情況下，得採用排除條款與豁免條款的選擇，無可避免地，此項設計將會使英國新法產生不一致與矛盾之狀況，一如過去 DPA 與歐盟資料保護指令在適用上產生的難題。長期而言，這些制度衝突雖可能在英國脫歐談判中解決，但在過渡時期中，由目前的發展看來尚無法得知該如何處理此種差異[43]。

肆、結論

英國政府對新法抱有很高的評價與期待，然或許因為立法過程過於倉促，也可能因為政府未就草案內容做通盤性的檢視與審核，導致外界批評聲浪不斷。本文認為英國國會在進入最終階段前，應廣納專家學者之建議仔細修改，不宜倉促立法，特別是在英國脫歐後，GDPR 將會成為英國內國法，與新資料保護法併行適用，兩者間若存在過多的

[38] Rebecca Hill, *UK Data Protection Bill lands: Oh dear, security researchers – where's your exemption?*, THE REGISTER, Sept. 14, 2017, https://www.theregister.co.uk/2017/09/14/messy_data_protection_bill_lands_in_parliament/ (last visited Nov. 9, 2017).

[39] Data Protection Bill, art. 31(7), (providing that: "'Third country' means a country or territory other than a member State.").

[40] Data Protection Bill, art. 71(1), (providing that: "A controller may not transfer personal data to a third country or to an international organisation unless…").

[41] Data Protection Bill, art. 72.

[42] Peter Ray Allison, *UK Data Protection Bill vs EU General Data Protection Regulation*, COMPUTERWEEKLY.COM, Nov. 1, 2017, http://www.computerweekly.com/feature/UK-Data-Protection-Bill-vs-EU-General-Data-Protection-Regulation (last visited Nov. 9, 2017).

[43] Alex Aisthorpe, *The Interplay between the Data Protection Bill and the GDPR*, ASHFORDS, Sept. 14, 2017, https://www.ashfords.co.uk/article/the-interplay-between-the-data-protection-bill-and-the-gdpr (last visited Nov. 9, 2017).

規範差異，將使國內機構與人民無所適從。草案已於 10 月 10 日完成二讀程序，並於 10 月 30 日進入委員會審議階段（committee stage），後續發展值得關注。

參考資料：

1. Eduardo Ustaran & Sam Choi, *UK's Draft GDPR Implementation Law: The Starting Point*, HOGAN LOVELLS, Sept. 27, 2017, http://www.hldataprotection.com/2017/09/articles/international-eu-privacy/uks-draft-gdpr-implementation-law-the-starting-point/?utm_source=dlvr.it&utm_medium=twitter (last visited Nov. 9, 2017).
2. Francis Aldhouse, *The UK Government Publishes the Data Protection Bill,* BIRD & BIRD LLP, Sept. 20, 2017, https://www.twobirds.com/en/news/articles/2017/uk/uk-government-publishes-data-protection-bill (last visited Nov. 9, 2017).
3. James Titcomb, *Data Protection Bill: How Will the New Laws Affect You?*, THE TELEGRAPH, Aug. 7, 2017, http://www.telegraph.co.uk/technology/0/data-protection-bill-will-new-laws-affect/ (last visited Nov. 9, 2017).