《高大法學論叢》

第 17 卷第 2 期（3/2022），頁 235-272

# 論歐盟第二支付服務指令下之個人資料保護

石佳立*

## 摘要

迅速成長的電子支付服務在全球金融科技發展中佔有一席之地，為加速歐盟單一電子支付市場，歐盟第二支付服務指令（PSD2）於 2018 年起落實於歐盟各國之國內法，持續加強歐元支付服務市場之整合，為開放銀行提供法律基礎，以平衡新支付服務機構與傳統支付機構之競爭及優勢，同時為了促進電子支付服務之發展，PSD2 認知個人資料之流通在多元化的電子支付市場下更盛以往，結合 GDPR 之規範，以確保支付服務使用者之資料保護以及支付安全。對於 PSD2 之架構下應如何適用 GDPR 之相關個人資料保護規定，歐洲資料保護委員會（European Data

* 東海大學法律系助理教授；美國威斯康辛州麥德遜分校法學博士。

投稿日期：06/25/2021；接受刊登日期：12/28/2021
責任校對：葉蕙禎、邱陽

Protection Board, EDPB）於 2020 年 12 月公布 PSD2 與 GDPR 交錯適用之指導原則（Guideline 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR），針對 PSD2 與 GDPR 適用上之主要議題，如 PSD2 如何落實 GDPR 規範下之支付服務使用者之資料自主權及資料可攜權，並針對具體同意權的行使、個人資料保護原則在電子支付交易環境下之適用、以及沉默第三人之資料保護，均有相當之分析。

鑑於我國在整合相關電子支付業者之監理而完成新修法之際，期本文能提供歐盟的立法設計為參考，重新檢視個人資料保護於我國電子支付環境下之適用，參酌 PSD2 與 GDPR 交錯適用建立在電子支付環境下之個人資料保護網，以增強消費者對於電子支付交易環境之信心及發展。

# Personal Data Protection Under the Legal Framework of the EU Second Payment Services Directive

Chia-li Shih**

## Abstract

The global electronic payment services market has grown rapidly in the area of financial technologies, commonly known as "FinTech." To facilitate the integration of the single payment market in Europe, the EU revised payment services directive (PSD2) has been implemented into EU members domestic laws since 2018. PSD2 provides a legal foundation for open banking in order to balance the competition between new payment services providers and conventional financial institutions. PSD2 also recognizes that personal data has been collected and used more aggressively during the transaction of electronic payment services. In addressing the significance of personal data protection, PSD2 ensures the payment services users' right to data portability and integrates with GDPR's legal framework. By defining the "explicit consent" and refining the application of the principles of data protection, PSD2 and GDPR have formed a protective net for personal data to ensure data

** Assistant Professor, The College of Law, Tunghai University; S.J.D., University of Wisconsin, Madison, U.S.A.

protection and portability.

Given that Taiwan has recently integrated and amended its laws governing electronic payment institutions, this research is intended to provide reference for Taiwan legislators in the consideration of examining the current personal data protection law and establish a legal framework of protecting personal data during the electronic payment process. Strengthening the personal data protection can significantly boost consumers' confidence on electronic payment services and therefore further the development of the electronic payment services industry.

# 論歐盟第二支付服務指令下之個人資料保護

石佳立

目錄



關鍵詞：第三方支付服務、歐盟第二支付服務指令、歐盟一般資料

保護規則、資料可攜權、開放銀行

Keywords: third party payment services, PSD2, GDPR, data portability, open banking.

# 壹、前言

多元化的電子付款制度為各國發展金融科技重要之一環，亦為電子商務以及跨國商務發展之重要助力，隨著無現金交易的普及化，增加電子付款之效率、平衡電子付款市場之競爭、保護使用者之權益以及減低電子支付交易之成本，雖為各國發展多元電子付款法制之主要考量，但為推動電子支付普及化，首重妥適保護支付服務使用者之個人資料以增加支付服務使用者之信心，使之進而改變傳統的支付習慣。歐盟於 2015 年 10 月 8 日通過新支付服務指令（Directive on Payment Services in the Internal Market, Amending Directive 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing Directive 2007/64/EC，以下簡稱 PSD2）[1]，以修正 2007 年所施行之第一支付服務指令（Directive on Payment Services in the Internal Market Amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC）[2]，PSD2 設定五目標以擴大支付服務

---

[1] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, L337/35 (Dec. 23, 2015). [hereinafter PSD2]. 對於 PSD2 的新規定，各會員國需於 2018 年 1 月 13 日前整合納入各會員國之國內法，目前對於 PSD2 整合，大多數的歐盟會員國均在 2018 年 1 月 13 日依該指令選擇整合國內法之措施，各國詳細的整合狀態，請見 National transposition measures communicated by the Member States concerning: Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, O.J. L. 337, 23.12.2015, p. 35–127, available at https://eur-lex.europa.eu/legal-content/EN/NIM/?uri= CELEX:32015L2366 (last visited 06/25/2021).

[2] Council Directive on Payment Services in the Internal Market Amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing

使用者之保護：第一、持續加強歐元支付服務市場之整合以及效率；第二、平衡新支付服務機構與傳統支付機構之競爭及優勢；第三、確保高度消費者保護以及支付安全；第四、鼓勵降低支付服務費用；第五、促進技術規格與其互用性，以期為電子支付市場帶來突破性之發展。為持續加強歐元支付服務市場之整合以及效率，PSD2 擴大適用支付服務指令之機構，納入兩項原本不受 PSD1 所規範的支付服務機構：支付起始服務（Payment Initiation Services Providers, “PISPs”）以及帳戶資料服務（Account Information Services Providers, “AISPs”）[3]，PSD2 藉由開放銀行之架構打破傳統相關支付服務市場之界定與疆域以活絡金融資訊服務市場之競爭[4]，更重要的是在增加市場競爭及支付服務種類的同時，強調消費者資料保護之重要性，PSD2 明文要求在處理支付服務使用者之個人資料時須受到 1995 年 10 月 24 日所制訂之資料保護指令（Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, “Data Protection Directive”）、各會員國內落實該指令之相關法令以及歐盟個人資料保護規章

---

Directive 97/5/EC, O.J. (L 319), O.J. L 319 5.12.2007, p. 1–36. [PSD1].

[3] PSD2 納入新型的第三方支付服務（Third Party Payment Services），依據 PSD2 第四條（3）該指令所適用的支付服務包括於其附件一所列之各項服務，其附件一服務之範圍除包括原本 PSD 所規範之範圍外，增列了支付起始服務（Payment Initiation Services Providers, “PISPs”）以及帳戶資料服務（Account Information Services Providers, “AISPs”）。PSD2 Art. 4 (3), 66, 67, & Annex.

[4] Simone Mezzacapo, *Competition Policy Issues in EU Retail Payment Business: the New PSD 2 Regulatory Principle of Open Online Access to Information from "Payment Accounts" and Associated "Payment transactions,"* 39 EUROPEAN COMPETITION L.R. 534, 537 (2018).

（Regulation (EC) No. 45/2001）之限制與適用[5]。然該 1995 年之資料保護指令（Data Protection Directive）於 2016 年經歐盟執委會（European Commission），向歐洲理事會（European Council）及歐洲議會（European Parliament）提出並通過「通用資料保護規則」（Regulation 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 (General Data Protection Regulation)，簡稱 GDPR）所取代[6]，GDPR 並於 2018 年 5 月 23 日生效取代資料保護指令並直接適用於歐盟地區[7]。

GDPR 除保留 1995 年資料保護指令之架構及基本原理原則[8]，更擴大個人資料之保護及適用之範圍、強化資料主體權並提高違反之罰則等，以達其立法目的：落實基本人權中之個人資料權保護以及確保個人資料於歐盟地區在此保護架構下自由的流通（free movement of personal data）[9]。

---

[5] PSD2 Art. 94; Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L 281, 23/11/1995 P. 0031 - 0050; Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000, on the Protection of Individuals with regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, O.J. L. 8/1, 12.1, 2001.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 95/46/EC (General Data Protection Regulation, hereinafter "GDPR"), O.J. L. 119, 4.5.2016, p. 1–88.

[7] 不同於資料保護指令，歐盟一般資料保護規則係為歐盟規章（EU Regulation），一經通過生效後，直接適用於歐盟地區。歐盟規章之制訂的法源來自於歐洲聯盟運作方式條約第 288 條之規定，Treaty on the Functioning of the European Union, Art. 288, 2012 O.J. (C 326) 1, 171-72.

[8] 李沛宸（2019），〈GDPR 當事人同意之實務採行建議〉，《商業法律與財金期刊》，2 卷 1 期，頁 70。

[9] W. Gregory Voss & Hugues Bouthinon-Dumas, *EU General Data Protection Regulation Sanctions in Theory and in Practice*, 37 SANTA CLARA HIGH TECH. L.J. 1, 7 (2020).

因此於 PSD2 結合 GDPR 之規範下，透過 PSD2 第 66 及 67 條之規定，提供開放銀行之法制基礎，落實 GDPR 之支付服務使用者之資料自主權及可攜權（Data Portability）[10]，使得資料主體得以同意決定個人資料於不同的金融機關或支付服務業者中蒐用與處理，同時為了保護消費者之金融資訊，在資料安全規格以及通訊上均設置通訊標準以及規格，以確保在開放銀行的同時不犧牲消費者之金融資料安全。

對於 PSD2 之架構下應如何適用 GDPR 之相關個人資料保護規定，歐洲資料保護委員會（European Data Protection Board, EDPB）於 2020 年 12 月公布 PSD2 與 GDPR 交錯適用之指導原則（Guideline 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR）[11]，本文以此指導原則為中心討論 PSD2 架構下 GDPR 相關的資料保護規定適用之主要議題，並釐清 PSD2 的支付體系供應鏈下所有參與者應如何遵守 GDPR，尤其針對新加入之 PISPs 及 AISPs 該如何在 PSD2 的架構下適用 GDPR 以保護支付服務使用者個人資料，藉由 PSD2 與 GDPR 之交錯，形成對於支付服務使用之消費者金融資訊之保護網，以確保消費者隱私權之保障，增加消費者對於新興電子支付之信心，進而加速電子支付之普及化及促進數位金融之發展。

我國為了加速金融科技及電子商務之發展，對於第三方支付法制於 2015 年通過電子支付機構管理條例，於 2016 年金融監督管理

---

[10] 所謂資料可攜性（Right to data portability），係指資料主體得不受個人資料控管者之妨礙，有結構性的、通常使用下接收、提供予其他資料控管人。GDPR Art. 20.

[11] European Data Protection Board (EDPB), Guideline 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR (12/15/2020), available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf. (last visited 06/25/2021).

委員會更發表了金融科技發展策略白皮書[12]，以 2020 年為期，從應用面、管理面、資源面、基礎面等 4 大面向，於六大核心領域：包括支付、保險、融資、募資、投資管理和市場供應等全力推動金融創新與發展，同時不斷在各種法規面上提供法制的架構以促進金融科技與電子商務之革新與發展[13]。

就電子支付方面，期許藉由政府及業者之推廣，提升電子支付於民間消費的比例由 26%到 52%，同時為積極發展開放銀行以及整合電子票證機構與電子支付機構、提供多元電子金融支付服務，於 2021 年 1 月 27 日完成電子支付機構管理條例之修正，新修正之電子支付機構管理條例將於 2021 年 7 月 1 日正式生效施行，開啟我國電子支付機構監管制度之新頁。在促進電子支付發展的過程，個人資料保護為增加消費者信心的重要關鍵，因此從歐盟之經驗，PSD2 結合 GDPR 共同架構對於電子支付環境之個人資料保護網，值得做為我國立法評估以及潛藏問題研究之借鏡，進而提供我國於發展開放銀行與平衡個人資料保護的法制參考。

## 貳、PSD2 架構下 GDPR 之適用與交錯

PSD2 為確保在多樣的新興電子支付服務下，消費者之資料保護不因開放銀行或新興電子支付服務提供者之加入而受到減損，結

---

[12] 金融監督管理委員會，〈金融科技發展策略白皮書〉，https://www.fsc.gov.tw/ch/home.jsp?id=517&parentpath=0，7，478（最後瀏覽日：06/28/2021）。

[13] 對於金融科技與電子商務之發展，鼓勵銀行業及電子商務業者積極發展新科技，並研發、申請電子商務相關之專利，我國銀行業也積極的在網路金融科技上積極的進行專利佈局以取得競爭的優勢，我國之智慧財產局亦具體舉例說明撰寫電子商務商業方法相關之多種不同類型之發明專利方法以符合專利適格性。關於我國關於電子商務商業方法之專利適格性請參酌周伯翰（2017），〈從台、美之法制分析電子商務商業方法之專利適格性〉，《中正財經法學》，14 期，頁 138-145。

合 GDPR 之法規，對於消費者之個人資料形成保護網，對於新興支付服務業者如何適用 PSD2 與 GDPR 結合之規範，EDPB 之 PSD2 與 GDPR 交錯適用之指導原則提出四個主要的爭點：一、新興支付服務業者如何適用 GDPR 之個人資料保護原則；二、如何在 PSD2 的架構下行使資料可攜權之「明確同意」；三、PSD2 對於沉默第三人之保護；以及四、PSD2 與 GDPR 結合下對於個人敏感性資料之保護，做出解釋，茲分論之：

## 一、PISPs 與 AISPs 蒐集、處理、利用個人資料時，應適用之 GDPR 與個人資料保護原則

### （一）PISPs 與 AISPs 需取得與處理支付服務使用者個人資料之合法事由

依據 GDPR 第 6 條 1 項之規定[14]，資料控管者需具有第 1 項所列 6 款合法性之事由之一始得蒐集、紀錄、或操作個人資料。其 6 款分別為一、取得資料主體之同意；二、為履行與資料主體所簽署之契約所必要者；三、遵守所負擔之法律義務所必要者、四、為保護資料主體或他人之重要利益所必要者；五、踐行公共任務所必要者；以及六、權衡資料主體之利益保護下為追求正當利益之目的所必要者[15]。究其規範，除經過資料主體者基於資料自主權所為之同意外，其他的合法性事由之判斷均需透過必要性之判斷以評估是否具備合法蒐用個人資料之合法性事由。

---

[14] GDPR Art. 6.

[15] 張陳弘（2019），〈GDPR 關於蒐用一般個人資料之合法事由規範〉，《月旦法學雜誌》285 期，頁 177。

然 GDPR 第 4 條（7）項中所稱之資料控管者[16]，係指對所蒐用之個人資料有權得獨立或與他人決定處理個人資料之目的及基本方式，如需蒐集的資料類型、範圍及存取的權限、在資料安全性受到侵害時，如遭不當竄改或竊取，得通知資料主體者[17]，並應確保資料主體權得行使之權利者[18]，因此在 PSD2 之架構下，PISPs 及 AISPs 為履行與電子支付服務使用者（資料主體）之支付服務契約，除了需遵守 PSD2 之規範於契約中明確與支付服務使用者之契約權利義務關係外，PSD2 於第三章更規範了定型化契約之基本條款與內涵，其中課予 PISPs 及 AISPs 對於所蒐集之資料必須於契約中明定使用支付服務所必要之資料範圍[19]，因此使 PISPs 及 AISPs 在電子支付服務契約下具有決定蒐用個人資料之範圍之權限，進而符合 GDPR 下之資料控管者之身分，應確保支付服務使用者之權益。

該契約之制訂雖提供支付服務業者取得支付服務使用者資料之合法性事由，然而歐洲資料保護委員會只特別就 GDPR 第 6

---

16 GDPR Art. 4(7).

17 Kyle Petersen, *GDPR: What (And Why) You Need to Know About EU Data Protection Law*, 31 UTAH B.J. 12, 14-15 (2018).

18 GDPR 對於處理個人資料主體分為資料控管者（Controller）以及處理者（Processor），於 GDPR 第 4 條（8）項中規範所謂資料處理者，與前述資料控管者不同，資料處理者僅為代資料控管者處理個人資料之法人、個人、公務機關或其他機構，與資料控管者對於資料處理之目的與保護具有控制權者不同。林玉書（2020），〈歐盟發布政府機關資料保護規則（Regulation (EU) 2018/1725 關於控管者、處理者和共同控管者概念之指導方針〉，《科技法務透析》，32 卷 9 期，頁 8；European Data Protection Board (EDPB), Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 3 (2020), available at https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf. (last visited 07/22/2021)；GDPR Art. 4(8).

19 PSD2 Art. 52.

條 1 項（b）款中所指蒐集及使用個人資料之必要性如何適用於 PSD2 之架構下做出解釋。GDPR 之第 6 條 1 項（b）款指出如基於履行與資料主體間之契約所必要者，自得蒐用該資料主體之個人資料。其中該必要性於電子支付服務市場下係指 PISPs 及 AISPs 需能證明如不取得並使用該個人資料即無法提供相關的支付服務始足當之，PISPs 及 AISPs 不得藉由單純在契約中表明使用資料之條款即認定其符合 GDPR 第 6 條 1 項（b）款之規定[20]。

因此結合 PSD2 與 GDPR 第 6 條 1 項（b）款之意涵，PISPs 及 AISPs 須視所提供服務之性質與內容，明確的載明其提供支付服務所必要而蒐集及使用之個人資料的範圍，並僅在該範圍內使用及處理支付服務使用者之個人資料[21]。始具備 GDPR 第 6 條 1 項（b）款所規範處理個人資料係為履行支付服務所必須之合法基礎[22]。

（二）PISPs 與 AISPs 蒐集、處理及使用支付服務使用者資料之原則

在 PSD2 與 GDPR 的結合適用下，PISPs 及 AISPs 於合法處理支付服務使用者之資料時，應依 GDPR 第 5 條之規定，對於所取得之資料，適用個人資料處理的七大原則，第一、為資料合法性、公正性、透明性原則[23]，意指於資料處理上應以合法、公正及透明的方式為之；第二、目的性限制原則，規範資料控管者在蒐集資料之目的上需特定、明確及合法[24]；第三、在蒐集範圍上，依資料最少蒐集

---

[20] European Data Protection Board, Guideline 2/2019 on the Processing Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to data subjects, (10/16/2019), available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en. (last visited 06/25/2021).

[21] EDPB, *supra* note 11, at 9.

[22] Simone Mezzacapo, *supra* note 4, at 541.

[23] GDPR Art. 5(1)(a).

[24] GDPR Art. 5(1)(b).

原則[25]，僅在適當、相關且限於處理目的所必要者始加以蒐集；第四、資料正確性原則[26]，對於個人資料之處理與儲存應維持其正確性，確保資料主體對於不正確的資料得以更正以維持其正確性；第五、資料儲存原則[27]，對於資料之儲存僅限於依其處理目的所需之時間內儲存；第六、資料完整性及保密原則[28]，指在資料處理上應確保其安全性採取適當之技術或組織上之措施，避免資料因受破壞而失其完整性；第七、資料控管者對其遵守原則規定須負舉證責任[29]。然在電子支付環境下由於敏感性資料，如支付服務使用者之金融資料，得於相關之支付服務機構間流通，EDPB 特別針對如何適用資料透明性原則及資料最少蒐集原則，以及資料的使用有明確之討論[30]，茲分述如下：

1.資料透明性原則與責任之課予

資料透明性原則（Transparency）以及課予資料控管者之責任為 GDPR 對於個人資料保護之基本原則，GDPR 第 5 條 1 項（a）款首先規定處理個人資料應以合法、公正及透明之方式為之[31]，對於所蒐集之資料應採取適當之方式於資料蒐集前或蒐集時提供資料主體 GDPR 第 13 及第 14 條所規範之相關資料，如資料控管者之聯繫方式及處理個人資料之目的及法律依據、該資料控管者之正當利益、或可能進行之資料移轉、提供主管機關必

---

25 GDPR Art. 5(1)(c).
26 GDPR Art. 5(1)(d).
27 GDPR Art. 5(1)(e).
28 GDPR Art. 5(1)(f).
29 GDPR Art. 5(2).
30 EDPB, *supra* note 11.
31 Lesley E. Weaver & Anne K. Davis, *The Interplay of the European Union's General Data Protection Regulation and U.S. E-Discovery - One Year Later, The View Remains The Same*, 29(1) COMPETITION: THE JOURNAL OF THE ANTITRUST, UCL AND PRIVACY SECTION 159, 160 (2019).

要之進階資料等資訊[32]，以確保個人資料處理之透明與公正。

對於合理的資料透明措施之執行，歐盟執委會設置有實施 GDPR 下個人資料透明性原則之指導原則（Article 29 Working Party Guidelines on Transparency under Regulation 2016/679，以下簡稱「透明性原則指導綱領」）[33]，對於如何在電子支付服務之環境下適用資料透明性原則，該指導綱領提出電子支付服務業者得結合不同之方式適用資料透明性原則，如將各種所須揭露的資料透過不同的隱私權保護政策及通知，分別提供不同的連結以供資料主體明確地知悉 GDPR 所規定第 13 條及第 14 條所要求揭露之資料[34]，而非透過單一連結提供全部資料，以避免因為對於資料疲勞而忽略所揭露的相關資料，始得達到資料揭露之有效性及目的。

該指導綱領更指出資料控管者亦得利用隱私權儀表版之功能（Privacy Dashboard）以單一窗口提供相關之隱私權資料，並使資料主體管理其隱私權之設定，如帳戶付款服務機構（Account Servicing Payment Services Provider, ASPSP）即得於該功能提供資料主體得行使撤回權之方式，資料主體權得透過該功能撤回對 PISPs 及 AISPs 之明確同意或行使資料可攜權移轉該資料予其他 PISPs 及 AISPs[35]。

對於以上落實 GDPR 資料透明性原則之責任，GDPR 第 5 條 1 項課予身為 GDPR 之資料控管者的電子支付服務機構須負擔舉證責任，證明其已採取適當之手段對於蒐集之資料的範圍、內

---

32 GDPR Art. 13 & 14.

33 The Working Party on the Protection of Individuals with Regard to the Processing of Personal data, Article 29 Working Party Guidelines on Transparency under Regulation 2016/679, WP260 rev.01 (04/11/2018), available at https://ec.europa.eu/newsroom/article29/items/622227 (last visited 06/25/2021).

34 *Id.* at 7, Pras. 8.

35 EDPB, *supra* note 11, at 23.

容、蒐集目的及資料主體之隱私權的風險控管及權利保護已盡相當之管理義務，同時在必要時應隨時更新其管理狀態以確保支付服務使用者之隱私權。

2.資料最少蒐集手段原則

對於支付服務使用者之資料蒐集，支付服務機構在 PSD2 適用 GDPR 第 5 條 1 項之規範下應採取最少蒐集手段原則[36]，意指僅就執行支付服務使用者所指示之特定支付服務必要範圍下始得蒐集其個人資料，同時 PSD2 亦要求 ASPSP 僅在經過支付服務使用者通知欲使用 PISPs 及 AISPs 時，始基於支付服務使用者之明確同意分享該個人資料予 PISPs 及 AISPs，因此適用資料最少蒐集原則於電子支付服務下，僅特定資料種類為執行支付服務所必須始為其蒐集範圍，PISPs 及 AISPs 不得蒐集超過該資料之範圍。

EDPB 更對支付服務機構適用資料最少蒐集手段原則提出範例，如支付服務使用者欲使用 AISPs 查詢其過去兩個月在其所開設之兩銀行帳戶下所有交易之資料，包括交易金額、收款人等資料，則基於資料最少蒐集手段原則，AISPs 在執行支付服務使用者之帳戶服務請求時，僅得在支付服務使用者所要求之特定資料種類下，如交易金額、收款人資料，向 ASPSP 請求相關的資料，對於未經請求之特定資料，如國際銀行帳戶代碼（International Bank Account Number,簡稱「IBAN」）等，即不得進行蒐集。

4.自動化建檔分析範圍之告知與限制

GDPR 第 4 條（4）項明訂建檔（Profiling）一詞係指對於所蒐集之個人資料以自動化方式處理、分析及評估與該資料主體相關之個人特徵，如分析或預測相關之經濟狀況、個人喜好、消費

[36] GDPR Art. 5(1).

行為等等，在 GDPR 的規範下，自動化建檔可作為支付服務決策之基礎或僅作為一般分析個人支付習慣之工具而不涉及決策事項，後者決策之作成亦得經支付服務使用者或因建檔分析之結果自動形成，例如基於自動化建檔後分析是否特定金融機構所提供之貸款為該支付服務使用者所需而同意該貸款或基於自動建檔之結果進行履行契約之行為等均為典型之範例[37]。

在 PSD2 架構下之支付服務機構在提供相關的支付服務過程中，使用自動化方式對於其所蒐集之個人資料進行評估分析以提供相關之服務甚至為支付服務中的一部份，如 AISPs 對於消費習慣、對象及金額進行分析報告[38]，因此支付服務機構業者應依據透明性原則指導綱領之規定落實 GDPR 之資料透明性原則[39]，揭露其如何透過自動化建檔分析在必要範圍內提供相關的支付服務，同時應遵守 GDRP 第 22 條之規定告知支付服務使用者有權不受因該自動化處理而產生之決策結果，包括透過自動化建檔（profiling）所做成之決策，如該決策對支付服務使用者發生法律效果或類似重大影響，支付服務使用者得不受該決策之拘束[40]。

---

[37] Brandon W. Jackson, *Cybersecurity, privacy, and artificial intelligence: an examination of legal issues surrounding the european union general data protection regulation and autonomous network defense*, 21 MINN. J.L. SCI. & TECH. 169, 193 (2020).

[38] 支付服務業者結合人工智慧（Artificial Intelligence）之技術對於支付服務使用者支付款行為進行自動建檔分析行為，以投其所好對支付服務業者推銷相關服務或產品之依據，因此 AI 技術的發展也成為電子支付服務中重要的一環，如同歐洲專利局（the European Patent Office）於 2017 年 12 月所公布的研究報告「專利與第四次工業革命」，其中提及第四次工業革命中的三大產業之一即為人工智慧（Artificial Intelligence），因此發展ＡＩ技術可否衍生專利，亦成為金融科技發展與競爭之兵家必爭之地。請參酌謝國廉（2020），〈論專利法對人工智慧之保護—歐美實務之觀點〉，《高大法學論叢》，15 卷 2 期，頁 7。

[39] EDPB, *supra* note 11, at 25-26.

[40] 在 GDPR 的規範下，自動化建檔可作為支付服務決策之基礎或僅作為一般分析

## 二、PSD2 架構下支付服務使用者行使資料可攜權所為之「明確同意」與 GDPR 之適用

### （一）PISPs 與 AISPs 因其提供支付服務而應具備 GDPR 之資料控管者及處理者之地位

PSD2 第 66 及 67 條賦予支付服務使用者得以明確的同意賦予 PISPs 及 AISPs 取得其金融個人資料之管道，該支付服務使用者之 ASPSP 即應依其明確之同意提供相關的金融資料予 PISPs 及 AISPs 以進行支付服務，該同意權之行使，使得 PISPs 及 AISPs，在提供支付起始服務或帳戶資料服務時，因管理、處理個人資料之角色而成為 GDPR 下第 4 條（7）項所稱之資料控管者（Controller）[41]或第 4 條（8）項下之處理者（Processor）[42]，進而應受 GDPR 關於控管者與處理者義務之適用。

### （二）PSD2 規範之「明確同意」（Explicit Consent）與 GDPR 之適用

如前述，PISPs 及 AISPs 於處理支付服務使用者之個人資料時，需結合 GDPR 第 5 條之規定並符合 PSD2 對於 PISPs 及 AISPs 取得支付服務使用者之金融資料之限制，於經支付服務使用者明確同意及提供支付服務必要之範圍內始得使用。PSD2 第 94 條第二項明文規定，所有支付服務機關僅得經支付服務使用者之「明確同

---

個人支付習慣之工具而不涉及決策事項，後者決策之作成亦得經支付服務使用者或因建檔分析之結果自動形成，例如基於自動化建檔後分析是否特定金融機構所提供之貸款為該支付服務使用者所需而同意該貸款，GDPR Art. 22.

41 GDPR 第 4 條（7）項下所指之控管者，係指單獨或與他人共同決定個人資料處理之目的與方法之自然人或法人、公務機關、局處或其他機構。GDPR Art. 4(7).

42 GDPR 第 4 條（8）項下所指之處理者，係指代控管者處理個人資料之自然人或法人、公務機關、局處或其他機構。GDPR Art. 4(8).

意」（Explicit Consent）下始得取得、處理、及儲存提供支付服務必要之個人資料[43]，同時第 64 條亦規定所有的交易需經過支付服務使用者之「同意」始得認定為經授權之交易[44]。其中 PSD2 所指明確同意之方式及內涵與 GDPR 所規定之「同意」（Consent）是否有不同且於實務上應如何適用？歐洲資料保護委員會特別針對此議題做出解釋。

首先歐洲資料保護委員會指出 PSD2 規範內之「明確同意」與 GDPR 中所指之「同意」之意涵不同[45]，GDPR 中所指之「同意」係指資料主體行使同意權之方式，GDPR 第 4 條（11）項對於同意之內涵做出解釋，指出 GDPR 下所指之「同意」[46]係指資料主體透過聲明或明確肯定之行為，所為自主性、具體、知情及確切之表示同意處理與其有關之個人資料，GDPR 同時在第 7 條第 1 項提供更進一步之保護，課予資料控管者對於取得資料主體之同意應具舉證之責任，控管者應證明其資料之處理係基於所資料主體之同意，且賦予資料主體得隨時對所蒐集處理之資料為撤回[47]。例外於資料主體為兒童時，對兒童提供資料社會服務時，為保護該兒童對於「同意」之內涵不具完全判斷之能力，因此 GDPR 第 8 條設置前條「同意」之例外規定，對於未滿 16 歲以下之兒童，僅在其法定代理人授權或同意的範圍內，始具合法之基礎。

然 PSD2 中所稱之「明確同意」係指資料主體於使用第三方支付服務前，先針對第三支付服務業者，如 PISPs 或 AISPs，所提出之支付服務契約上具體載明第三方服務機構於提供第三方支

---

43 PSD2 Art. 94(2).
44 PSD2 Art. 64.
45 EDPB, *supra* note 11, at 14.
46 李沛宸，同前註 8，頁 76-79。
47 GDPR Art. 7.

付服務時將蒐集、使用其個人資料之範圍及使用目的之內容，經明確的告知以及瞭解後，再就該個人資料蒐集及處理之條款所為之同意[48]，第三方支付服務業者僅於符合該明確同意之範圍下始得取得該資料主體之個人資料。

探究 PSD2 與 GDPR 所規範之「同意」定義與要件，雖係從不同的層面去規範及保護資料主體之資料自主權，強調個人資料之流通需經過資料主體之同意，然在 PSD2 的架構下與 GDPR 之交錯適用下，資料主體於 PSD2 架構下所為之同意仍應符合 GDPR 下同意之定義，以具備處理個人資料之合理性。換言之，於支付服務使用者選擇第三方支付服務之時所為之資料取得權之同意，應符合 GDPR 第 4 條（11）項所規定之要件[49]，1.需於意思自由下所給予；2.該同意需就資料取得之特定範圍及目的為充分瞭解後所為之同意；3.該同意需為具體而非模糊概括的同意；4.該同意應以書面或具體的行為為之，以確認資料主體在明確瞭解使用第三方支付服務對其個人資料之影響後所做出有實質意義之同意，進而落實對於資料主體之個人資料保護。

## 三、PSD2 對沉默第三方（Silent Party）資料之保護

相對於第三方支付服務使用者依 PSD2 及 GDPR 之規定，得透過明確的同意行使其資料自主權，在使用第三方支付服務過程中受到個人資料之保護，第三方支付服務使用者之相對人的個人資料於第三方支付服務使用者使用該服務時，將不可避免的經第三方支付服務使用者所揭露，以完成第三方支付之程序，此過程

---

48 EDPB, *supra* note 11, at 14.
49 GDPR Art. 4 (11).

中並無該第三方相對人得介入施予同意、或由該第三方支付業者需事先與該第三方相對人成立支付服務契約以取得該第三方之個人資料之程序，來保護該第三方相對人之個人資料，典型的例子即為第三方支付服務使用者於使用第三方支付服務時，於付款之過程中需提供收款人之個人資料以完成相關之付款行為[50]。在該付款程序過程中該收款人的個人資料即在未事先經該收款人的同意下提供予第三方支付服務業者，且經第三方支付服務業者於提供相關支付服務之過程中為使用。因此對於該沉默第三方資料之保護，該如何賦予同等的保護，亦為 PSD2 與 GDPR 交錯適用下的重要課題。

對於該沉默第三方之資料保護，本於 PSD2 第 94 條 1 項之規定，亦應受到 GDPR 之規範而受到保護。GDPR 第 5 條 1 項（b）款特別載明資料蒐集之目的限制原則，亦即對於資料蒐集目的須特定、明確及合法，且不得更為超出該等目的以外之處理[51]，更有甚者，GDPR 第 6 條 1 項（f）款亦規範資料控管者於處理第三方資料僅限於合法目的下之必要範圍內始得為之，同時應平衡該第三人之個人資料權益及自由，如該第三人之個人資料利益應超越所欲處理之交易利益及目的，該第三人之個人資料權益應優先受到保護，否則該資料控管者即不得蒐集或處理該第三人之個人資料。

適用 GDPR 於 PSD2 的支付服務架構下，PISPs 或 AISPs 在履行支付服務契約之過程中，對於所取得之沉默第三方個人資料亦僅限於在履行支付服務契約之範圍內，且在履行該支付契約必

[50] EDPB, *supra* note 11, at 16.
[51] GDPR Art. 5 (1)(b).

要之有限目的下，始得蒐集或使用該第三人之個人資料，同時應遵行 PSD2 所規範之安全通訊規格，對於沉默第三人之個人資料亦應建立資料安全保護的機制並且不得加以儲存[52]，以維護該沉默第三人個人資料之權益，如需對於第三人之個人資料做進一步之利用，更應在原始蒐集及處理個人資料之目的下使用，始得符合 PSD2 及 GDPR 之保護規範。

## 四、PSD2 與 GDPR 交錯下對個人敏感性資料（Sensitive Data）之保護

敏感性資料涉及個人之種族、宗教、性向、政治傾向或哲學信仰等具有高度個人識別性之資料，考量這類敏感性資料具有高度私密性，且需高強度之隱私權保護，各國對於該類資料多採取高度保護之措施與規範。在使用支付服務過程中，第三方支付服務業者所處理之支付服務使用者之支付交易資料，其本質上雖不當然屬於敏感性資料，然就特定金融交易資料中，時有得自支付服務使用者交易之情況，進而推知或使第三方支付服務業者取得或處理相關的敏感性資料的情形，典型的範例為支付服務使用者如對特定宗教或政黨為捐獻，或可從其捐獻中推知其宗教或政黨之傾向。更甚者，AISPs 在提供相關支付服務資料服務的過程亦可從使用者經常性之交易，透過建檔（Profiling），以大數據自動化分析處理該使用者之個人資料，從中分析或預測該使用者之敏感性資料及特定傾向，因此考量敏感性資料在 PISPs 及 AISPs 的支付服務或帳戶資料服務提供過程中可能造成敏感性資料之洩漏，PSD2 與 GDPR 之適用即提供第三方支付服務使用者敏感性資料之保護。

---

[52] PSD2 Art. 66(3)(g) & 67.

PSD2 第四條第 32 項就 PSD2 中所稱「敏感性付款資料」（sensitive payment data）[53]做出定義，所謂「敏感性付款資料」係指得用以施行詐騙手段之個人安全驗證資料。分析該定義，其定義與 GDPR 第 9 條所規範之特殊個人資料類型顯有不同。GDPR 第 9 條所稱「敏感性資料」係指種族或民族起源、政治意見、宗教或哲學信仰或貿易聯盟會員資格之個人資料、以及基因資料、特別用以識別自然人之生物特徵的識別資料、關於健康或關於自然人之性生活或性傾向的資料，對於此類的敏感性資料，除非符合 GDPR 第 9 條第 2 項所列舉的（a）~（j）款之規定，否則第三方支付業者不得處理該敏感性資料。

從 GDPR 第 9 條 2 項所列舉之十款從規範之本質上而言，其第 9 條 2 項（b）~（f）及（h）~（j）款性質上並不適用 PSD2 支付服務[54]，因此得適用於 PSD2 支付服務交易處理敏感性資料之基礎，僅限於第 9 條 2 項（a）款及（g）款。PSD2 第 66 條及 67 條均規範在授權交易時應經支付服務使用者之明確同意，依 GDPR 第 9 條 2 項（a）款，除歐盟法或該會員國法特殊規定，資料主體不得以「同意」排除處理敏感性資料之限制外，支付服務業者須經資料主體之明確同意始得處理個人敏感性資料，因此 PSD2 支付服務業者於處理支付服務使用者之敏感資料時，為確實遵守 GDPR 之規定，歐盟資料保護委員會特別建議 PISPs 及 AISPs 應先依 GDPR 第 35 條之規定[55]，進行資料保護影響評估，評估其支付服務所使用之新科技處理方式，對於敏感性資料可能處理之範圍、本質、使用情況、以及目的，衡量該處理

---

53 PSD2 Art.4 (32).
54 EDPB, *supra* note 11, at 19.
55 *Id.*

方式對於該支付服務使用者之權利及自由可能造成之風險，並於交易程序下採取特定的保護處理措施，並對於處理該敏感性資料前取得支付服務使用者之明確同意，始得符合於 GDPR 以及 PDS2 之規定。

## 參、由 PSD2 及 GDPR 之結合反思在我國新修正之電子支付管理條例下之個人資料保護

電子支付制度已逐漸的改變大眾的支付習慣，因其使用之便利性，在歐盟單一市場下，支付服務使用之用戶迅速的成長中，如歐盟統計在 2018 年較 2017 年，非現金交易在歐元市場成長 7.9%，並逐年增加中，足見非現金交易對資金之流通、支付之效率以及金融交易之發展扮演著重要的角色。觀之民眾支付習慣的改變，便利性、支付效率、以及個人資料之保護更成為主要推動之因素。我國在推動電子支付多元化以及普惠金融之際[56]，對於現行的電子支付機構管理條例，進行大幅的修正，新條例即將於 2021 年 7 月 1 日生效施行，觀其修正之目的係為整合電子支付機構與電子票證機構之二元化管制，透過擴大電子支付機構之業務範圍，增加跨機構小額金融匯兌服務[57]，以提升電子支付服務之多樣化及便利性，達到電子支付之普及化。觀之我國民眾之消費習慣，縱電子支付之比例逐年增加，但相較於其他亞洲國家電子化

[56] 金融監督管理委員會於 2016 年提出「電子支付比率五年倍增計畫」，目標於五年內將電子支付金額佔民間消費支出之比率，從 2015 年的 27.64%，倍增至 2020 年的 52%。林惠君（2020），〈電子化支付逆勢成長〉《財金資訊季刊》，98 期，頁 11。

[57] 蔣念祖、戴凡芹（2019），〈電子支付機構管理條例修正草案評析〉，《萬國法律》，228 期，頁 83。

支付之比重，我國使用電子支付之比率仍相對較低[58]，現金支付仍為我國主要之消費支付工具，其中一主因即是顧慮電子支付之安全性以及個人資料之保護，然在此次修法中多著重於電子支付機構之監管，對於個人資料於電子支付環境下之保護，並未如同 PSD2 設有結合個人資料保護法之立法架構，反而於立法理由中提及將使用者個人資料之利用回歸個人資料保護法適用[59]，然我國的個人資料保護法，僅就非公務機關對於個人資料之蒐集與使用為概括性保護原則之規定，並無如同 GDPR 賦予電子支付服務使用者對於個人資料具有可攜權，如何在電子支付服務交易過程適用個人資料保護法以保護電子支付服務使用者之個人資料即為重要之議題。因此鑑於在我國電子支付發展之過程，電子支付基礎硬體制度、消費者使用現金之習慣以及消費者對於個人資料保護之考量，向來影響電子支付之普及化，為增加消費者對於新興電子支付環境之信心，PSD2 與 GDPR 的結合，在電子支付環境下所建立的個人資料防護網極具參考價值。

## 一、資料自主權與資料可攜權之落實

PSD2 對於推動電子支付服務的重要措施之一即為開放銀行提供取得個人資料之法制基礎，透過貫徹 GDPR 所保護之資料主體的資料可攜權，降低電子支付機構之市場競爭障礙。於傳統的金融帳戶服務機構，消費者之金融資料向來被視為重要資產[60]，傳統

---

58 林惠君，同前註 56，頁 13。

59 請參閱電子支付機構管理條例修正草案總說明。

60 Deloitte UK, How to Flourish in an Uncertain Banking and PSD2 9, available at https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-open-banking-and-psd2.pdf. (last visited 04/20/2021).

金融帳戶機構得透過大數據，分析並取得消費者之金融消費資料，進而針對其偏好及需求提供金融服務，以取得競爭之優勢，並透過與支付服務使用者間之保密契約增加第三方支付服務機構進入市場之困難[61]。在 PSD2 及 GDPR 第 20 條的規範下，支付服務使用者得自主決定何支付服務機構得以蒐集使用其資料、資料蒐集之範圍及時間的長短，如此的資料自主權及可攜權之賦予使得支付服務使用者取得主導的權利[62]，進而得決定在何支付服務機構間分享其個人資料，同時藉由傳統金融帳戶服務業者間開放式之應用程式介面（Applications Programming Interface, API）之建置，使電子支付服務機構在取得支付服務使用者之具體同意後，得要求帳戶服務機構（傳統的金融帳戶服務機構）需依支付服務者之具體同意開放相關的金融資料予電子支付服務機構[63]，一方面確保支付服務使用者對於自身金融資料之主控權，二方面使得電子支付服務機構得排除傳統金融機構將所持有之支付服務使用者之金融資料資產化而產生之市場競爭障礙，更進一步創造電子支付服務機構與與帳戶服務機構整合的機會以提出多元化之服務，因而得降低電子支付機構之市場競爭障礙，並活化電子支付服務市場。

我國為順應國際開放銀行之潮流，金管會亦 2018 年 10 月邀請銀行公會、財金資訊公司、財團法人金融聯合徵信中心及銀行業者針對開放銀行之模式及實務上之操作交換意見，並由財金資訊公司為主導，於 2019 年 4 月籌組開放 API 研究暨發展委員

---

61 Stanley M. Besen, *Competition, Privacy, and Big Data*, 28 CATH. U. J. L. & TECH. 63, 64 (2020).

62 Lindsay A. Seventko, *GDPR: Navigating compliance as a United States Bank*, 23 N.C. BANKING INST. 201, 222 (2019).

63 Wolfgang A. Maschek, *EU Regulatory and Supervisory Trends for FinTech Operators in Europe - A Policy Perspective*, 19(4) FINTECH L. REP. NL 3, 1 (2016).

會，對於開放銀行之規劃著重於 API 技術之整合與資料安全標準之統一，研擬相關開放銀行之 API 技術及資安標準[64]，目前金管會之立場係鼓勵公會自律，而非透過立法強制[65]，然 PSD2 提出不同的思考方向，開放銀行之架構如果僅限於支付服務提供業者間自行之整合，仍得可能因為產業競爭的壁壘，而無法得到真正開放的效益，然如果透過法規之強制，並以支付服務使用者為中心，透過資料可攜權之行使，使電子支付服務提供者為取得競爭之先機，在電子支付過程中提出多樣化的電子支付服務以吸引消費者，實能達到活化電子支付服務之競爭與動能[66]。

更有甚者，開放銀行既為我國金融科技發展重點之一，此次修正電子支付機構管理條例之目的亦希望擴大電子支付機構之業務範圍，增加跨機構小額金融匯兌服務、提供多元化的電子支付服務，以增加電子支付市場之競爭力，為達成此目標，金融資料之開放扮演不可或缺之角色，因此更需要透過個人資料保護法之規範強化電子支付服務使用者之資料主導權，透過資料可攜權更能促進支付服務機構間之競爭，並強化電子支付服務機構對於個人資料保護之義務[67]。此次修正電子支付機構管理條例並未提供消費者資料可攜權之合理及保護措施之法規架構，加上我國個人資料保護法亦無如同 GDPR 與 PSD2 對於消費者資料可攜性為相關之規定，對於強化消費者資料之保護以及金融資料跨機構流通

64 臧正運（2019），〈從國際發展趨勢論我國推動開放銀行應有之思考〉，《金融聯合徵信》，34 期，頁 12。

65 蔡昌憲、彭冠蓉（2021），〈開放銀行之管制政策研究-以歐盟與英國的經驗為中心〉，《月旦法學雜誌》，313 期，頁 82。

66 孫鈺婷（2020），〈數位經濟下的個人資料流通-以開放銀行為例〉，《科技法律透析》，32 卷 12 期，頁 33。

67 同前註，頁 89。

以促進電子支付市場之競爭，似嫌不足。因此如能參考歐盟 PSD2 結合 GDPR 對開放銀行下所造成之資料流通之保護架構於我國個人資料保護法下規範資料可攜權之法源，落實資料自主權，使開放銀行回歸以支付服務使用者為中心。

## 二、強調個人資料於電子支付交易環境下之保護

EDPB 所公布對於 PSD2 與 GDPR 交錯適用之指導原則，詳盡的指出在 PSD2 的架構下，於電子支付服務交易的每個階段 GDPR 所建置的個人資料保護應如何適用？包括支付交易服務前階段，如何強化支付服務使用者之資料可攜權，到交易中階段如何透過定型化契約從立法控制電子支付所可能產生對於支付服務使用者之風險，並結合 GDPR 形成明確同意之內涵，及建立資料處理之相關原則，以確保支付服務使用者在 PSD2 架構下之資料保護。

由 EDPB 之指導原則中可知電子支付服務之過程對於個人資料之保護有其特殊性，需針對其特殊性在 PSD2 的架構下適性的適用 GDPR 之個人資料保護規定，以強化消費者保護及對於電子支付之信心，然此次電子支付機構管理條例，著重於電子支付機構之整合、服務範圍之擴大及監理之彈性，將個人資料保護的部分回歸個人資料保護法之適用，然我國個人資料保護法對於電子支付中個人資料之利用、處理及取得之特殊性，尤其於第三人資料保護部分之規定仍付之闕如，為落實隱私權保護之意旨，值得參酌 EDPB 之指導綱領關於 PSD2 之架構下於電子支付服務交易下如何於每個交易階段落實個人資料保護法之規定而審酌個人資料保護法之相關架構是否足以因應電子支付服務之多元化發展。

## 三、沉默第三方之資料保護

電子支付交易之過程，資料主體之資料保護依 PSD2 及 GDPR 之規定，均適用資料透明原則、明確同意制度、及目的性限制原則，同時亦有相關之契約規範以作為保護之基礎且將其保護擴及交易過程中之第三人，PSD2 及 GDPR 更考量到在電子支付服務過程中，所涉及之資料主體，除了當事人外，亦涉及沉默之第三人，如支付服務使用者欲支付之相對人，該相對人於電子支付過程中，電子支付服務業者並無與之訂立相關契約之機制，或取得該相對人明確同意之機制，因此本於個人資料保護之原則，PSD2 與 GDPR 亦限制電子支付服務業者僅得於履行支付契約必要之合目的性限制下始得蒐集、利用該相對人之資料，並課予資料控管者需平衡第三方之個人資料權與交易之利益與目的，而決定蒐集第三人資料之正當性。

對於該沉默第三人之資料保護，不論在此次修正之電子支付機構條例或是個人資料保護法中均未加以提及，觀之個人資料保護法第 19 條規範對於個人資料之蒐集或處理需於特定目的內，經符合第 19 條各款之一的規定始得為之。進而個人資料保護法第 20 條規定對於個人資料之利用，需於蒐集之特定目的內利用，除有但書之情事外始得為特定目的外之利用。檢視個人資料保護法第 19 條各款及第 20 條電子支付服務業者對於沉默第三人之資料蒐集與處理利用，並未符合第 19 條之所列各款情事，除第 19 條 3、4、6 款於性質上不適用外，因電子支付服務交易過程中，沉默第三人並未與支付服務機構具有契約或類似契約之關係，因此無第 19 條 5 款之適用；同時電子支付服務並無相關的機制使沉默第三人行使同意權，故第 19 條 5 款亦無適用之機

會；加上在電子支付服務之過程中，所涉及之沉默第三人之個人資料多涉及敏感之金融資料，如第三人之帳戶資料以作為匯兌收款之用，該資料並非公開之資料，或得取自一般可得之來源，故第 19 條 7 款亦無適用之機會，因此最後或得之依據為第 19 條 8 款，然於第三人支付服務過程中蒐集、處理或利用沉默第三人之資料如何判斷是否對於當事人權益無侵害，因其資料之敏感性高，應有其明確之標準。

再者，金管會對於電子支付機構管理條例設置電子支付機構業務管理規則，於該規則第 7 條之規定中僅規定電子支付機構應依使用者之支付指示，進行支付款項移轉作業，對於使用者之支付指示需記載收款方之相關身份資料，並應屏蔽個人使用者之姓名[68]，但對於該收款方之相關個人資料保護之規定亦付之闕如，鑑於實務上時見沉默第三方之個資經洩露之爭議[69]，且此次電子支付機構管理條例修正之重點之一係增加跨機構之金流服務，對於金流服務中第三人資料之保護更顯其重要性，GDPR 第 6 條 d 款及 f 款明確課予資料控管人需評估第三人之重大利益及正當利益以做為資料蒐集合法性之基礎，值得作為修正我國個人資料保護法第 19 條及 20 條之參考，以涵蓋對於第三人之保護。

---

[68] 請參酌金管會一百零八年七月二日金融監督管理委員會金管銀票字第 10802720010 號令修正發布第 2、6、7、10、12、15、20、20-1、24、26、27 條條文；增訂第 5-1、12-1 條文及條文對照表。

[69] Line pay 一卡通於 2018 年 9 月上路時，曾發生交易之第三方個人資料暴露之爭議，該事件起因於國人常用的通訊軟體 Line，提供 Line Pay 一卡通之轉帳功能，然在使用轉帳的功能時、實際轉帳付款前，即得看到對方之真實姓名以及其電子支付帳戶帳號，由於 Line 得讓所有的用戶單方面的透過搜尋 ID，直接加入好友，因此得輕易獲取第三人之個人姓名資料，引發個資洩露之疑慮。

# 肆、結語

電子支付服務的多元化，降低消費者對於現金之依賴，大幅減低交易之成本，更增加金融服務之便利性與金流之效率，大量的消費者交易資料在支付過程中快速的流通與蒐用，為加速電子支付服務市場發展、強化多方當事人個人資料之保護得增加消費者對於電子支付之信心，對於普惠金融之推動，有相當之助益。PSD2 與 GDPR 的結合適用，提供個人資料之保護在電子支付交易環境下防護網之藍圖，並提供我國在發展數位金融以及整合相關電子支付業者之監理而完成新修法之際數項值得參考之方向：

第一、PSD2 與 GDPR 在強化支付服務使用者之資料主體權及資料可攜權下，不僅一方面增加支付服務使用者對於個人資料之主導權，使支付服務使用者得依其需求決定個人資料之流通及使用以增加支付服務之效益，另一方面在 PSD2 的強制規定下更促使開放銀行之機制，降低傳統金融機構之資料壁壘所造成之競爭障礙，PSD2 與 GDPR 之結合使開放銀行產生真正的效益，並回歸以使用者為中心之思想。如前述我國亦積極的發展開放銀行，以期加速數位金融之發展，然開放銀行之建置不僅僅在技術上維持安全性及隱密性，更須在個人資料保護上使資料主體取得自主權，透過資料可攜權的強化，使支付服務使用者能實質的活化金融服務產業，但在新修正的電子支付機構管理條例中，第 31 及 32 條僅著重於電子支付機構交易資料之保密及安全性標準，然關於個人資料保護之議題，僅於立法理由中提及回歸於個人資料保護法為規範，於個人資料保護法僅規定同意權的行使，並未如 GDPR 積極的賦予資料可攜權，使個人資料得因支付服務使用者之主導而流通。因此如參酌 PSD2 與 GDPR 之機制，增

修個人資料保護法，積極賦予資料主體權之資料可攜權，同時於電子支付機構管理條例增訂開放銀行之強制基礎，使電子支付機構與相關帳戶服務機構間得因支付服務使用者之主導及參與，發生實際的效益，如此不僅有助於增加消費者對電子支付之信心，更能使在發展多元化電子支付服務上降低市場進入障礙，達到普惠金融之目標。

第二、於非傳統交易之電子支付環境下適用個人資料保護法需考量傳統個人資料保護原則之適用性，尤其是電子支付交易下所流通的資料多為高敏感性之個人財務資料，在數位金融的發展下，透過建檔（Profiling）方式，分析支付服務使用者之交易習慣、對象、方式，更使電子支付業者掌握相當商業價值之個人資料，因此更值得檢視電子支付交易流程中是否產生個資保護之漏洞，我國個人資料保護法對於依自動建檔方式僅定義於第 2 條第２款作為蒐集個人資料之方式，對於如因自動化建檔方式而發生決策，因而對資料主體造成法律效果之結果，並無相關之規定，在迎向人工智慧時代，如何調整傳統個人資料保護原則於電子支付服務中之自動化建檔所造成之個人資料保護影響及效力，有賴個人資料保護法與電子支付機構條例增訂如 GDPR 第 22 條之強制規定以及設置對於自動化建檔行為之限制，以落實個人資料於電子支付交易流程中之保護。

第三、由於在電子支付交易過程中個人資料經廣泛的蒐用，同時所涉及的個人資料甚至包括未使用電子支付服務之第三人，因此更有必要針對電子支付服務可能造成對個人資料保護之衝擊為審視，PSD2 與 GDPR 之結合分別對電子支付中可能蒐用的當事人以及第三人之資料，強化的沉默第三人之保護，以解決電子支付所造成的個資問題。在我國強調電子支付市場之發展與電子支付機構之整合之際，值得參酌 PSD2 與 GDPR 之設計，對於電

子支付服務使用可能涉及到的沉默第三人之個人資料，檢視個人資料保護法如何因應多樣化的支付服務可能帶來對於支付服務交易所涉及個人資料保護之衝擊，而為特殊化之規定，由於對該沉默第三人而言，其個人資料係由支付服務使用者所提出，並未經該沉默第三人之明確同意，因此是否考慮擴大對於當事人之個人資料保護於在該情況下延伸至該沉默之相對人，實為我國電子支付市場競爭發展下值得考量的課題，以達到電子支付發展與個人資料保護之平衡。

# 參考文獻

## 一、中文部分

李沛宸（2019）。〈GDPR 當事人同意之實務採行建議〉,《商業法律與財金期刊》,2 卷 1 期，頁 67-96。

周伯翰（2017）。〈從台、美之法制分析電子商務商業方法之專利適格性〉,《中正財經法學》,14 期，頁 47-164。

林玉書（2020）。〈歐盟發布政府機關資料保護規則（Regulation (EU) 2018/1725）關於控管者、處理者和共同控管者概念之指導方針〉,《科技法務透析》,32 卷 9 期，頁 7-9。

林惠君（2020）。〈電子化支付逆勢成長〉,《財金資訊季刊》,98 期，頁 11-15。

孫鈺婷（2020）。〈數位經濟下的個人資料流通-以開放銀行為例〉,《科技法律透析》,32 卷 12 期，頁 30-37。

張陳弘（2019）。〈GDPR 關於蒐用一般個人資料之合法事由規範〉,《月旦法學雜誌》,285 期，頁 174-190。

臧正運（2019）。〈從國際發展趨勢論我國推動開放銀行應有之思考〉,《金融聯合徵信》,34 期，頁 4-12。

蔡昌憲、彭冠蓉（2021）。〈開放銀行之管制政策研究-以歐盟與英國的經驗為中心〉,《月旦法學雜誌》,313 期，頁 76-96。

蔣念祖、戴凡芹（2019）。〈電子支付機構管理條例修正草案評析〉,《萬國法律》,228 期，頁 83-96。

謝國廉（2020）。〈論專利法對人工智慧之保護—歐美實務之觀點〉,《高大法學論叢》,15 卷 2 期，頁 1-38。

## 二、英文部分

Besen, Stanley M. (2020). *Competition, Privacy, and Big Data*. Catholic University Journal of Law and Technology. 28, 63-88.

Deloitte UK, How to Flourish in an Uncertain Banking and PSD2 (2017), available at https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/ financial-services/cz-open-banking-and-psd2.pdf (last visited 04/20/2021).

European Data Protection Board (EDPB), Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR (2020), available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf (last visited 06/21/2021).

European Data Protection Board (EDPB), Guidelines 07/2020 on the concepts of controller and processor in the GDPR (2020), available at https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (last visited 06/26/2021).

European Data Protection Board, Guideline 2/2019 on the Processing Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to data subjects (2019), available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en (last visited 06/25/2021).

Jackson, Brandon W. (2020). *Cybersecurity, Privacy, and Artificial Intelligence: an Examination of Legal Issues Surrounding the European Union General Data Protection Regulation and*

*Autonomous Network Defense*. Minnesota Journal of Law, Science & Technology, 21, 169-207.

Maschek, Wolfgang A. (2016). *EU Regulatory and Supervisory Trends for FinTech Operators in Europe - A Policy Perspective*. FinTech Law Report NL 3, 19, 1-9.

Mezzacapo, Simone (2018). *Competition Policy Issues in EU Retail Payment Business: the New PSD 2 Regulatory Principle of Open Online Access to Information from "Payment Accounts" and Associated "Payment transactions*." European Competition Law Review, 39, 534-544.

Petersen, Kyle (2018). *GDPR: What (And Why) You Need to Know About EU Data Protection Law*. Utah's Business Journal, 31, 12-16.

Seventko, Lindsay A. (2019). *GDPR: Navigating compliance as a United States Bank*. North Carolina Banking Institute, 23, 201-229.

The Working Party on the Protection of Individuals with Regard to the Processing of Personal data, Article 29 Working Party Guidelines on Transparency under Regulation 2016/679, WP260 rev.01 (2018), available at https://ec.europa.eu/newsroom/article29/items/622227 (last visited 06/25/2021).

Voss, W. Gregory & Bouthinon-Dumas, Hugues (2020). *EU General Data Protection Regulation Sanctions in Theory and in Practice*. Santa Clara High Technology Law Journal, 37, 1-96.

Weaver, Lesley E. & Davis, Anne K. (2019). *The Interplay of the European Union's General Data Protection Regulation and U.S. E-Discovery-One Year Later, the View Remains the Same*. Competition: The Journal of the. Antitrust, UCL and Privacy Section, 29, 159-168.