新加坡資料共享法制環境建構簡介

新加坡資料共享法制環境建構簡介

資訊工業策進會科技法律研究所
2019年12月31日

壹、事件摘要

如何有效運用資料創造最大效益為數位經濟（Digital Economy）重點，其中資料共享（data sharing）是有效方法之一。新加坡自2018年以來推動「資料共享安排」機制（Data Sharing Arrangements, 下稱DSAs）與「可信任資料共享框架」（Trusted Data Sharing Framework），建構資料共享環境，帶動國內組織[1]資料經濟發展與競爭力。

貳、重點說明

自從2014年新加坡政府推行「2025智慧國家（Smart Nation）」以來，即積極鋪設國家數位經濟建設，大數據資料分析等數位科技發展為其重點，預估2022年60%國內生產總值將與數位經濟有關[2] 。其中，希望透過資料共享促進組織、政府、個人三方間資料無障礙流通，降低蒐集、處理與利用成本，創造更多合作機會進行創新應用，因此從法制面、環境面與技術應用層面打造完善的資料共享生態系統（data sharing ecosystem）[3]。

然而依據《個人資料保護法》（Personal Data Protection Act 2012，下稱個資法）第14條以下規定，組織蒐集、處理與利用個人資料應取得當事人同意，除非符合第17條研究目的等例外情形。由於資料共享強調可將資料進行多節點快速傳遞近用，使資料利用價值最大化，因此若依據個資法規定每次共享皆須事前獲得當事人同意，將使近用成本增高並間接造成資料流通產生障礙。因此為因應國家政策與產業需求，新加坡個人資料保護委員會（Personal Data Protection Commission, 下稱個資委員會）依據個資法第62條所賦予的豁免權（exemption），個人或組織可在遵循個資委員會訂定的規則下，依照個案給予組織免除個資法部分規範[4] ，而DSAs機制即是一種[5]。

DSAs是由個資委員會於2018年設立的沙盒（sandbox）計畫，如組織所進行的共享模式是在特定群體並範圍具體明確，同時不會造成個人有負面影響等情事，可在不須經個人同意下進行資料共享[6]。並且，為進一步提升組織與消費者間信任，2019年6月個資委員會與資訊通信媒體發展局（Info-Communication Media Development Authority of Singapore，下稱資通發展局）共同推出「可信任資料共享框架」指南建議，由政府擔任監管角色，組織只要符合指南建議方向，如遵循法律、達到一定資料技術應用品質與實施資安與個資保護措施下，可以進行個人與商業資料之共享，DSAs機制是共享方法之一。以下簡述新加坡個資法規範、指南建議與DSAs機制運作方式。

圖1：資料共享環境建構

資料來源：新加坡資通發展局

一、新加坡個人資料保護法規範

在沒有個資法第17條所列之例外情形下，依據第14條以下規定，組織如近用個人資料應獲得個人同意，同時應符合目的使用及通知義務，尤其應給予個人可隨時撤回同意之權利[7]。

同時組織應根據個人要求，提供近用個人資料之方法、範圍與內容，以及更正錯誤資料權利[8]。並且組織必須任命資料保護官（Data Protection Officer, DPO）隨時向大眾提供通暢的個資聯絡管道，來確保個資透明性與完整性[9]。

在資料保護措施上應有合理安全的資安防護技術，以保障資料不被未經授權近用的風險。當使用目的不在時，需妥善保留或予以去識別化，同時如須境外轉移資料時，境外之資料保護措施應至少與新加坡個資法規範標準相同[10]。

二、免除同意之DSAs機制

DSAs機制是由個資委員會於2018年設立的沙盒（sandbox）計畫，也就是組織可透過申請免除資料共享前必須獲得個人同意之規範。然而如

組織擬向個資委員會申請DSAs機制，必須符合三個條件[11]：

1. **共享範圍需在特定群體、期間與組織內**：即只限定在具體特定的應用情境內，若超出申請範圍，例如分享至其他非申請範圍的組織，則須再經過個資委員會批准[12]。
2. **近用目的需具體明確**：即資料共享必須應用於特定且明確目的，如以「社會研究目的」作為申請則範圍過大不夠明確[13]。
3. **近用資料對於個人不會有不利影響，或公共利益大於個人利益**：例如共享目的不是直接用於銷售或存在合法利益，或是共享本身具備公共利益且明顯大於個人可預見的（foreseeable）不利影響，此時個資委員會可考慮同意組織申請免除[14]。

三、建立以信任為基礎之資料共享模式

雖然取得DSAs機制免除同意可以使資料近用方式更為簡便，然而在進行資料共享前，仍應有完善的技術品質與資安保護措施，因此在「可信任資料共享框架」指南建議中，組織應透過法律遵循、導入AI或區塊鏈等新興技術，並具備相應資安保護措施來建構可信任的資料共享環境，實際步驟可分為以下四階段[15]：

圖2：可信任資料框架

資料來源：新加坡資通發展局

第一階段為「資料共享建構」[16]，由組織自行評估存有的商業或個人資料是否具共享價值與潛在利益，並要如何進行共享，例如資料共享方式屬於雙邊（bilateral）、多邊（multilateral）或是分散式（decentralized，又稱「去中心化」）。以及資料種類有哪些，如主資料（master data）、交易資料、元資料（metadata）、非結構化資料（unstructured data）等。組織可將資料共享方式、種類依據無形資產（intangible asset）評價方式，即市場法（market approach）、成本法（cost approach）與收入法（income approach）三種評價方法進行評價，來衡量共享之價值性。除資料價值判斷外，組織必須自行評估自身組織與將來之合作夥伴是否有足夠能力管控共享之資料，包括是否具備一定技術能力的資安與資料保護措施等。

第二階段為「法律規範考量」[17]，即決定哪些資料可以進行共享，從規範面檢視個資法、競爭法與銀行法等是否有例外不得共享規定，例如信用卡號碼或個人生物識別資訊不得共享。若資料共享類型不會對個人造成不利影響或具備公共利益，並有通知（notification）個人給予選擇退出（opt-out）的機會，組織可依個案申請DSAs機制之豁免。同時另外鼓勵組織向IMDA申請資料保護信任標章（Data Protection Trustmark, DPTM）認證，透過認證機制使消費者更能信任組織運用其個人資料[18]。

第三階段為「技術組織考量」[19]，包含組織是否有能力建立資安風險管理與個資侵害之因應措施，是否有即時將資料安全備份技術，並針對不同傳輸技術如有線/無線網路、遠端存取（VPN）、應用程式介面（API）、區塊鏈等區分不同資安防護與風險管理能力。

最後一階段為「資料共享操作」，當已準備進行資料共享時，需再次檢視是否已符合前三個階段，包含透明性、責任義務、法律遵循、近用資料方式與取得目的外利用同意等[20]。

參、事件評析

個人資料視為21世紀驅動創新的重要價值，我國部會亦開始討論「個資資產化」的可能[21]。面對數位經濟時代來臨，有效運用數位科技將潛藏個人資料的大數據進行加值利用，不僅有利組織與創新發展，更可回饋消費者享有更好的產品與服務。

新加坡政府以資料共享作為數位經濟發展重點方向之一，在具備一定程度技術能力、資安保護措施與組織控管之條件下，可向主管機關申請免除個人同意之規範。透過一定法規鬆綁讓資料利用最大化以創造產業創新價值，同時依據主管機關要求的保護措施，使消費者信賴個人資料不會遭受不當利用或侵害。DSAs機制與「可信任資料共享框架」指南之建立，適時調適個人資料保護規範與資料應用間的衝突，並提供組織進行資料共享之依循建議，作為推動該國數位經濟發展方針之一。

[1]組織（organisation）依據新加坡個人資料保護法（Personal Data Protection Act 2012）第2條泛指個人、公司、協會、法人或團體。

[2]INFOCOMM MEDIA DEVELOPMENT AUTHORITY 【IMDA】, *Trusted data sharing framework* (2019), at 7, https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf (last visited Sep. 11, 2019).

[3]*id.*

[4]Personal Data Protection Act 2012 (No. 26 of 2012) §62, "The Commission may, with the approval of the Minister, by order published in the Gazette, exempt any person or organisation or any class of persons or organisations from all or any of the provisions of this Act, subject to such terms or conditions as may be specified in the order."

[5]Data Sharing Arrangements, PDPC, https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Exemption-Requests/Data-Sharing-Arrangements (last visited Dec. 1, 2019).

[6]*id.*

[7]IMDA, *supra* note 2, at 31; Personal Data Protection Act 2012 (No. 26 of 2012) §14, 16, 20.

[8]*id.* Personal Data Protection Act 2012 (No. 26 of 2012) §21.

[9]IMDA, *supra* note 2, at 31.

[10]*id.* at 32. Personal Data Protection Act 2012 (No. 26 of 2012) §24-26.

[11]*id*.

[12]PERSONAL DATA PROTECTION COMMISSION【PDPC】, *Guide to Data Sharing* (2018), at 14, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Data-Sharing-revised-26-Feb-2018.pdf (last revised Oct. 3, 2019).

[13]*id.*

[14]*id.*

[15]PDPC, *supra* note 4. at 28.

[16]*id*. at 21, 23-25.

[17]*id*. at 35

[18]*id*. at 30. Data Protection Trustmark Certification, IMDA, https://www.imda.gov.sg/programme-listing/data-protection-trustmark-certification (last visited Sep. 26, 2019).

[19]*id*. at 41-47.

[20]*id*. at 50-51.

[21]林于蘅，〈自己的個資自己賣！國發會擬推「個資資產化」〉，聯合新聞網，2019/06/17，https://udn.com/news/story/7238/3877400（最後瀏覽日：2019/10/1）。

相關連結

- Data Sharing Arrangements
- Data Protection Trustmark Certification
- 自己的個資自己賣！國發會擬推「個資資產化」

相關附件

- Guide to Data Sharing (2018) [pdf]
- Trusted data sharing framework (2019) [pdf]

吳昌鴻
法律研究員 編譯整理

上稿時間：2020年04月

文章標籤

推薦文章