Consent and Personal Data: Charting the Differences between the PDPA and GDPR

I. Introduction

Over the past few years, techniques to refine and process data have been developed and honed. Whether it is developments in machine learning or the internet-of-things, the invention of these technologies has made data a valuable and strategic commodity.[1] Given the importance and value of data to commercial operations, this has led to the mass collection of user data by corporation and institutions to facilitate their activities.[2]

However, despite the rising importance and value of data, institutions and corporations may not adequately protect such data in event of a breach. Therefore, to better understand what steps Singapore has taken to solve this issue, this article begins with introducing how Singapore's Personal Data Protection Act[3] has dealt with the issue of consent, specifically focusing on the concepts of deemed consent and the exceptions to consent.

Following which, we will then provide perspective on the efforts that Singapore in relation to data protection by comparing the local PDPA with the renowned General Data Protection Regulation,[4] which had been studied[5] in the drafting of the Personal Data Protection (Amendment) Bill 2020.[6] The GDPR is a uniform data security law adopted by the European Parliament in April 2016, replacing an outdated Data Protection Directive from 1995. The GDPR applies to both companies that have and do not have a presence in an EU country so long as they process personal data of European residents.[7] In particular, our analysis focuses on how the GDPR has implemented the idea of consent, comparing it with that of deemed

---

1 The Economist, "The world's most valuable resource is no longer oil, but data" (6 May 2017) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (accessed 26 January 2021)

2 Thomas H. Davenport, "Competing on Analytics" Harvard Business Review January 2006.

3 Personal Data Protection Act 2012 (Act 26 of 2012) ("PDPA").

4 General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR").

5 *Singapore Parliamentary Debates, Official Report* (2 November 2020) vol 95 (S Iswaran, Minister for Communications and Information).

6 Personal Data Protection (Amendment) Bill 2020 (Bill 37 of 2020).

7 Information Commissioner's Office, "Frequently asked questions" <https://ico.org.uk/for-organisations/business/guide-to-the-general-data-protection-regulation-gdpr-faqs/> (accessed 29 December 2020).

consent and the exceptions to the requirement of consent in the PDPA.[8] This article then concludes by shedding light on the potential reasons which have led to the differences between the PDPA and the GDPR, and what this might mean for companies trying to comply with both.

II. Consent in the amended Personal Data Protection Act[9]

A. Collection, use & disclosure of personal data

Under the PDPA, personal data is data that can identify an individual.[10] This definition means that a broad range of information, from health records to banking details can constitute personal data.

Unless where "required or authorised under [the PDPA] or any other written law",[11] consent if required for the collection, usage or disclosure of an individual's personal data.[12] Situations where consent is not needed as laid out in the PDPA are as follows:

(a) when it is in the "vital interests of individuals";[13]
(b) when it is of "matters affecting public";[14]
(c) when there is "legitimate interest";[15]
(d) where "business asset transactions" are involved;[16] and

---

8 Hannah Yee Fen Lim, "GDPR matchup: Singapore's Personal Data Protection Act" (14 June 2017) <https://iapp.org/news/a/gdpr-matchup-singapores-personal-data-protection-act/> (accessed 29 December 2020).

9 See also the two Advisory Guidelines that have been published by the Personal Data Protection Commission on the key concepts in the PDPA and an elaboration on selected topics. Personal Data Protection Commission Singapore, "Advisory Guidelines on Key Concepts in the Personal Data Protection Act" (1 October 2021) <https://www.pdpc.gov.sg/Guidelines-and-Consultation/2020/03/Advisory-Guidelines-on-Key-Concepts-in-the-Personal-Data-Protection-Act> (accessed 11 January 2022). Personal Data Protection Commission Singapore, "Advisory Guidelines on the Personal Data Protection Act for Selected Topics" (4 October 2021) <https://www.pdpc.gov.sg/Guidelines-and-Consultation/2020/02/Advisory-Guidelines-on-the-Personal-Data-Protection-Act-for-Selected-Topics> (accessed 11 January 2022).

10 *Supra* n 3, at s 2.

11 *Id*, at s 13(a).

12 *Id*, at s 13(b).

13 *Id*, at First Schedule Part 1.

14 *Id*, at First Schedule Part 2.

15 *Id*, at First Schedule Part 3.

16 *Id*, at First Schedule Part 4.

(e) when it is for "business improvement purposes".[17]

(1) Consent

Consent can be express, such as through a written agreement.[18] Consent can be deemed as well.[19] Consent is deemed as given if an individual "voluntarily provides the personal data to the organisation for that purpose",[20] or if "it is reasonable that the individual would voluntarily provide the data".[21] Additionally, consent will now be deemed given if it is "reasonably necessary for the conclusion of the contract" between the individual and the organisation.[22]

Even if consent is given, there are limitations as to how personal data can be collected, used, or disclosed. When providing a product or service, consent cannot be given beyond what is reasonable to provide the product or service.[23] Consent also cannot be obtained or attempted to be obtained by providing false or misleading information with respect to the collection, use, or disclosure of personal data, or by using deceptive or misleading practices.[24]

(2) Exceptions to consent

While the amendments now allow for more exceptions to consent, such exceptions are typically subject to limitations. Moreover, any collection, use or disclosure of personal data without consent is always subjected to a "reasonable" standard, which is the test of what a reasonable man would do in the circumstances.[25] Hence, for organisations whose activities relate to personal data, it will be prudent to obtain express consent when possible. Organisations that need to obtain consent can do so by express means as previously mentioned or by notification.[26]

(a) Vital interest of individuals

---

17 *Id*, at First Schedule Part 5.

18 *Id*, at s 13(a).

19 *Ibid*.

20 *Id*, at s 15(1)(a).

21 *Id*, at s 15(1)(b).

22 *Id*, at s 15(3).

23 *Id*, at s 14(2)(a).

24 *Id*, at s 14(2)(b).

25 *Id*, at s 3, s 11(1). See also *Jump Rope (Singapore)* [2016] SGPDPC 21 at [11].

26 *Id*, at s 15A.

The first exception to consent pertains to whether the collection, use, and disclosure is in the vital interest of individuals.[27] The definition of "vital interest" uses a narrow approach, where vital interest relates to the protecting the life of individuals.[28] Under the PDPA, the collection, use or disclosure of personal data is in the vital interest of individual if it "is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual",[29] or the organisation is unable to obtain consent in a timely way and has reasonable grounds to believe that that there is such an emergency.[30] Consent is likewise not needed if the collection, use or disclosure of personal data is merely to contact the next-of-kin or a friend of any injured, ill or deceased individuals.[31]

(b) Matters affecting public

The second exception to consent is whether the personal data is of a matter affecting the public.[32] This exception covers a myriad of issues. For instance, consent is not needed if the personal data about an individual is publicly available; is of national interest; is solely for artistic or literary purposes; is solely for archival or historically purposes provided the personal data is reasonably not too sensitive; or solely for news activity by a news organisation.[33]

(c) Legitimate interest

The third exception to consent pertains to whether "the collection, use or disclosure of personal data is in the legitimate interest of the organisation" collecting, using, or disclosing the personal data or of the legitimate interest of another person.[34] Pursuant to the amendments, the concept of "legitimate interest" would cover a large array of matters. For instance, such interest could be for evaluative purposes; to aid in investigations and proceedings; to recover or pay debts; to aid individuals in procuring legal services; to aid the preparation of a credit report; to allow the organisation to provide a service for an individual; or for employment relations.[35]

---

27 *Id*, at First Schedule Part 1.

28 *Supra* n 4, at Recital 46.

29 *Supra* n 3, at First Schedule Part 1 s 2.

30 *Id*, at First Schedule Part 1 s 3.

31 *Id*, at First Schedule Part 1 s 4.

32 *Id*, at First Schedule Part 2.

33 *Ibid*.

34 *Id*, at First Schedule Part 3.

35 *Id*, at First Schedule Part 3 s 2 – s 10.

However, for an exception of legitimate interest to be allowed, the legitimate interests cannot outweigh any adverse effect on the individual whose personal data is being collected, used, or disclosed.[36] To ensure this, organisations have to conduct assessments to determine if the legitimate interest indeed outweigh the adverse effects.[37] Moreover, the organisation must provide the individual with reasonable access to the personal data being collected, used, or disclosed by them while identify and implement reasonable measures that deal with the adverse effects.[38]

(d) Business asset transactions

The fourth exception pertains to organisations dealing with business asset transactions. This exception applies if personal data of an individual is collected, used, or disclosed for such transactions.[39] However, this exception does bear many limitations. First, the collection, use or disclosure of personal data can only be done in a way that is necessary for the business asset transaction to proceed.[40] Moreover, if an individual's personal data has been disclosed, the disclosing organisation must notify that individual of this disclosure.[41] Additionally, if the transaction ultimately does not proceed, the organisation must destroy or return the individual all of his personal data collected.[42]

(e) Business improvement purposes

The last exception pertains to personal data that is collected, used, or disclosed for business improvement purposes. For an organisation's collection, use or disclosure of an individual's personal data to be covered by this exception, such collection, use or disclosure must confer a benefit on that individual or other customers. This benefit could constitutes improving or developing goods and services for that individual.[43] It could also be to help another organisation that the individual is a customer of to learn and understand the behaviour and preferences of that individual or others in relation to the goods and services provided by either

---

36 *Id*, at First Schedule Part 3 s 1(1)(b).

37 *Id*, at First Schedule Part 3 s 1(2)(a).

38 *Id*, at First Schedule Part 3 s 1(2)(b) and s 1(3).

39 *Id*, at First Schedule Part 4 s 1(1) and s 2(1).

40 *Id*, at First Schedule Part 4 s 1(3)(a) and s 2(2)(a)(i).

41 *Id*, at First Schedule Part 4 s 1(4)(c) and s 2(3)(b).

42 *Id*, at First Schedule Part 4 s 1(5) and s 2(4).

43 *Id*, at First Schedule Part 5 s 1(2)(a).

organisation.[44] However, this exception is only valid provided the relevant purposes and benefits cannot be reasonably achieved without the collection, use or disclosure of the personal data.[45]

III. EU GDPR vs PDPA

A. Deemed consent

Unlike the PDPA, the concept of deemed consent is not statutorily encoded in the GDPR, which in fact requires consent to be "unambiguous, explicit, expressed and be freely given".[46] Instead, the GDPR lays out six legal bases for processing personal data, serving as exceptions in the European Union, where processing of personal data is generally prohibited.[47] Organisations, which are termed "data controllers" under the GDPR, are required to identify one of the six bases as their legal basis for data processing. The six grounds are as follows:[48]

(a) Where the individual "has given consent to the processing of personal data for one or more specific purposes";[49]

(b) Where "processing is necessary for the performance of a contract";[50]

(c) Where "processing is necessary for compliance with a legal obligation to which [the individual] is subject";[51]

(d) Where "processing is necessary in order to protect the vital interests of [the individual] or of another natural person";[52]

(e) Where "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller";[53] and

---

44 *Id*, at First Schedule Part 5 s 1(2)(d).

45 *Id*, at First Schedule Part 5 s 1(3)(a) and s 1(4).

46 *Supra* n 4, at Article 4(11).

47 *Id*, at Article 6.

48 *Ibid*.

49 *Id*, at Article 6 s 1(a).

50 *Id*, at Article 6 s 1(b).

51 *Id*, at Article 6 s 1(c).

52 *Id*, at Article 6 s 1(d).

53 *Id*, at Article 6 s 1(e).

(f) Where "processing is necessary for the legitimate interests pursued … except where such interests are overridden by the interests of fundamental rights and freedoms of [the individual]".[54]

B. Exceptions to consent

There are two key differences between the GDPR and the PDPA with regard to the alternatives to consent that businesses can rely on.

(1) Wider ambit of exceptions to consent

First, the potential exceptions to consent for organisations to rely on under the PDPA are far broader than those laid out in the GDPR.[55] Previously, the exceptions listed in the PDPA covered three of the six legal bases in the GDPR - namely situations when it is in the vital interests of individuals,[56] where it involves matters affecting the public[57] and when it is a business asset transaction.[58]

Following the introduction of the First Schedule in the amended PDPA, the ambit of the exceptions to consent under the PDPA has since widened to an even greater extent[59] with the introduction of the legitimate interests exception.[60] In addition, the business improvement exception, which is not provided for in the GDPR, had also been introduced.[61]

Examining the business improvement exception helps provide some insight towards reconciling the differences between the approaches taken by Singapore and the EU with regard to the issue of consent. In the Second Reading of the Personal Data Protection (Amendment) Bill 2020, Minister for Communications and Information, Mr S Iswaran, had shared how the

---

54 *Id*, at Article 6 s 1(f).

55 *Id*, at Article 5(1)(b).

56 *Supra* n 3, at First Schedule Part 1. See also *supra* n 4, at Article 6 s 1(d).

57 *Id*, at First Schedule Part 2. See also s*upra* n 4, at Article 6 s 1(e).

58 *Id*, at First Schedule Part 4. See also s*upra* n 4, at Article 6 s 1(b).

59 *Ibid*.

60 *Id* First Schedule Part 3. See also s*upra* n 29, GDPR Article 6 s 1(f).

61 *Supra* n 3, at First Schedule Part 5 s 1(2)(a).

purpose of the business improvement exception was to "support innovation and introduction of new services" and had been drafted in recognition of the commercial realities in Singapore.[62]

The same notion is reinforced when we observe the difference in aims between the PDPA and the GDPR. In Singapore, alongside the protection of consumers' personal data, [63] another key aim of the PDPA is to "support Singapore's ambition to be an innovation and commercial hub". [64] This is as compared to the EU, where there is a greater focus on "protect[ing] fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data" by offering a more detailed legislation[65] on the protection of personal data as laid out in Article 8 of the EU Treaty on Fundamental Rights.[66]

The different foci shed some light on why the PDPA has comparatively more liberal standards for companies on the issue of consent and why moving forward, it is crucial for the PDPA to pave a path separate from the GDPR.

(2) Difference in form

The second difference lies in the way these alternative options are framed. Unlike the GDPR which explicitly provides for the six aforementioned legal grounds, the PDPA has been drafted in a manner which provides that exceptions to consent may rise where "required or authorised under [the PDPA] or any other written law".[67] The comparatively more general manner in which s 13(b) was drafted signals a possible intention to allow for exceptions to consent beyond those stated in the First Schedule insofar as these exceptions have been statutorily encoded.

IV. Conclusion

---

62 *Supra* n 5.

63 *Ibid*.

64 Ministry of Communications and Information and Personal Data Protection Commission, *Amendments to the Personal Data Protection Act and Spam Control Act Passed* (2 November 2020) at para 7.

65 Integritetsskydds Myndigheten, "The purposes and scope of the General Data Protection Regulation" <https://www.imy.se/other-lang/in-english/the-general-data-protection-regulation-gdpr/the-purposes-and-scope-of-the-general-data-protection-regulation/> (accessed 17 February 2021).

66 Charter of Fundamental Rights of the European Union (2012/C 326/02) Article 8.

67 *Id*, at s 13(b).

Through our brief comparison of the PDPA and the GDPR with regard to their consent provisions, we have been able to observe the motivations and the direction in which Singapore's PDPA is heading. In particular, the recent amendments to the PDPA sought to ensure the continued relevance of the balance attained between the development of data-driven technologies, such as big data analytics, and the safeguarding of consumer interests.[68] However, only time will tell regarding Singapore's stance in light of the development of the digital economy.

[68] *Supra* n 5.