Singapore Law Review
Juris Illuminae Vol 10 (2018/19)

THE EUROPEAN UNION'S GDPR – A VIEW FROM SINGAPORE

This article was written in July 2018, two months after the GDPR came into force. At the time of publication, the GDPR has not seen any further amendments.

ONG KYE JING

INTRODUCTION

The European Union's [EU] long-awaited General Data Protection Regulation[1] [GDPR] finally came into effect on 25 May 2018. The product of a decade-long legislative endeavour,[2] the GDPR promised a much–needed update to the EU's Data Protection Directive [DPD],[3] the latter having been introduced when less than 1% of EU citizens were Internet users.[4]

The GDPR has gotten off to an exciting start. Complaints were filed within an hour of it coming into force,[5] as were billion-dollar lawsuits within the first 24 hours.[6] Consumers were subjected to a flurry of emails as businesses scrambled to secure fresh consent.[7] This anxiety is

---

[1] EC, *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 (General Data Protection Regulation),* [2016] OJ, L119/1 [GDPR].

[2] Paul de Hert & Vagelis Papakonstantinou, "The new General Data Protection Regulation: Still a sound system for the protection of individuals?" (2016) 32 CLSR 179 at 180.

[3] EC, *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] OJ, L 281/31.

[4] EC, Press Release, IP/12/46, "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses" (25 January 2012), online: Press Release Database <http://europa.eu/rapid/press-release_IP-12-46_en.htm> For a survey on the development of EU data protection laws, see generally Bart van der Sloot, "Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation" (2014) 4(4) IDPL 307.

[5] Jeewon Kim Serrato et al, "One week into GDPR – what you need to know" (4 June 2018), *Data Protection Report* (blog), online: <https://www.dataprotectionreport.com/2018/06/one-week-into-gdpr-what-you-need-to-know/>.

[6] David Hart QC, "$8 billion lawsuits started on GDPR day" (31 May 2018), *UK Human Rights Blog* (blog), online: <https://ukhumanrightsblog.com/2018/05/31/8-billion-lawsuits-started-on-gdpr-day/>.

[7] Alex Hern, "Most GDPR emails unnecessary and illegal, say experts", *The Guardian* (21 May 2018), online: <https://www.theguardian.com/technology/2018/may/21/gdpr-emails-mostly-unnecessary-and-in-some-cases-illegal-say-experts>.

understandable: the GDPR empowers supervisory authorities to impose fines as high as EUR 20,000,000 or 4% of an organisation's total worldwide annual turnover, whichever is higher.[8] Prior to this, maximum penalties had only amounted to EUR 3,000,000 in France and EUR 300,000 in Germany.[9]

An equally significant change is the GDPR's theoretically–universal territorial reach. Applying the principle of *lex loci solutionis*, data controllers that (i) offer goods or services to individuals in the EU, or (ii) monitor their behaviour within the EU, could face obligations under the GDPR *despite* not being physically or legally established in the EU.[10] Processors (or data intermediaries) that handle such data may also face obligations, albeit of a more limited nature.

In other words, several Singapore–based organisations will now face dual obligations under both the GDPR and Singapore's Personal Data Protection Act[11] [PDPA]. This article attempts to briefly but critically compare the approaches taken under each regime, with a focus on controllers' obligations. Broadly, it will explore the themes of consent, purpose limitation and notification, and accountability.

CONSENT

Under the PDPA, controllers cannot collect, use or disclose personal data[12] without the data subject's consent.[13] Under the GDPR, consent retains its privileged position. In fact, the GDPR

---

[8] GDPR, art 83(6).

[9] As highlighted in Paul Voigt & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Cham, SUI: Springer International, 2017) [GDPR Practical Guide] at 209, n 45, citing the relevant French and German statutes.

[10] GDPR, art 3. See also EC, European Data Protection Board [EDPB], "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)" (16 November 2018), online: <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf>.

[11] *Personal Data Protection Act 2012* (No 26 of 2012, Sing) [PDPA].

[12] Similarly defined under both PDPA, s 2 and GDPR, art 4, but note in particular GDPR, arts 8–9. Where personal data is obtained from a child below 16–years–old in relation to information society services, art 8 of GDPR, carves out special rules. Art 9 of GDPR, identifies special categories of personal data that are regarded as more sensitive and as requiring greater protection. The absence of similar protections for the personal data of children in Singapore has been regarded as a "significant gap": see Simon Chesterman, "From Privacy to Data Protection" in Simon Chesterman, ed, *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World*, 2nd ed (Singapore: Academy Publishing, 2018) 13 [*Chesterman*] at paras 2.63–2.67.

[13] PDPA, s 13.

goes further to stipulate that consent must be a "freely given, specific, informed and unambiguous indication of a data subject's wishes".[14] Each element deserves some scrutiny.

To an extent, the second and third requirements – of "specific" and "informed" consent" – are nothing new vis-à-vis the PDPA. Consent must be "specific" in that the controller's exact purpose(s) for data processing must be explicitly delineated and sufficiently granular. And for consent to be "informed", consent requests need to be communicated in clear and plain language, separately from other matters, and together with other relevant information like the controller's identity, the data subject's right to withdraw consent, and the possible risks of data transfers.[15]

One notable difference with the GDPR is that consent must also be "freely given". Building upon the procedural ingredients above, this injects a substantive element to the test for consent. Data subjects must have a "genuine [and] free choice" and be able to "refuse or withdraw consent without detriment".[16] A statutory presumption against freely–given consent will likely apply where (i) parties experience clear power imbalances, like in employment relationships, or (ii) separate consent cannot be given for different data processing operations.[17] Accordingly, controllers should (i) identify an alternative basis for processing where an imbalance exists, and (ii) seek standalone consent for each class of processing operations.

Finally, consent must amount to an unambiguous indication of the data subject's interests. This requires a clear statement or affirmative act from the data subject;[18] silence, inactivity, and pre–ticked boxes do not suffice.[19] One might query whether such an exclusionary rule against apparent omissions unduly places form over substance. In this regard, the PDPA's discretionary position towards opt–out clauses is perhaps preferable. Singapore's Personal Data Protection Commission [PDPC] recognises, for example, that a data subject who leaves a clause stating "tick here if you

---

[14] GDPR, art 4(11). Under certain circumstances, such as where special categories of personal data are concerned, an even higher standard of "explicit consent" is required: see EU Article 29 Data Protection Working Party, "Guidelines on consent under Regulation 2016/679" (WP259 rev.01) (10 April 2018) [WP29 Guidelines on Consent] at 18.

[15] WP29 Guidelines on Consent at 11–18.

[16] GDPR, rec 42.

[17] GDPR, rec 43. See also Lukas Feiler, Nikolaus Forgó & Michaela Weigl, *The EU General Data Protection Regulation (GDPR): a commentary* (Woking, Surrey: Globe Law and Business, 2018) at 88; WP29 Guidelines on Consent at 10.

[18] WP Guidelines on Consent at 15.

[19] GDPR, rec 32.

do not wish your personal data to be provided" unticked, but who otherwise meticulously fills out and submits the remainder of an application form, could reasonably be said to have consented.[20]

Two further observations should be made:

First, the theme of fairness which underlies these requirements appears to feature even more prominently in the GDPR's recitals. In particular, rec 42 stipulates that a declaration of consent "should not contain unfair terms",[21] in line with Council Directive 93/13/EEC[22] on unfair terms in consumer contracts. Unfortunately, it is unclear how much weight ought to be placed on rec 42. Recitals are not substantive provisions in their own right, but mainly serve to explain the basis for legislation. Moreover, the GDPR does not expound on the manner and extent to which these provisions, which apply predominantly to the sale of goods, are to be transposed to data protection. Any attempt at directly transplanting these considerations into Singapore might entail an even further leap, given that European consumer protection standards and the law on unfair terms in Singapore might not be doctrinally compatible.[23] In short, rec 42's practical significance remains to be seen.

Second, unlike the PDPA, the GDPR rejects the notion that consent can be deemed. Therefore, even if an individual voluntarily provides her personal data, for purposes she was aware of, and in circumstances where providing such data is reasonable, this alone would not constitute valid consent under the GDPR.[24] A controller seeking to legitimise such data processing should instead rely on another basis for processing.[25]

---

[20] Personal Data Protection Commission Singapore, "Advisory Guidelines on Key Concepts in the Personal Data Protection Act" (27 July 2017) [PDPA Key Concepts] at para 12.10. See also *Re YesTuition Agency* [2016] SGPDPC 5 generally for a relatively liberal approach to opt–out clauses (there, the PDPC did not object to the existence of a broadly–worded, opt–out clause).

[21] *Supra* note 16.

[22] EC, *Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts*, [1993] L 95/29 [*Directive 93/13/EEC*].

[23] Compare the breadth of the definition and illustrations of "unfair terms" in *Directive 93/13/EEC*, art 3 and Annex, with Singapore's *Unfair Contract Terms Act* (Cap 396, 1994 Rev Ed Sing), ss 2–4.

[24] PDPA, s 15(1). See also PDPA Key Concepts at para 12.28.

[25] In fact, organisations are already being advised to bypass the consent requirement altogether by considering alternative bases: GDPR Practical Guide at section 4.2.1.

LAWFUL BASES FOR PROCESSING

Apart from explicit consent, a controller can justify the collection, use or disclosure of data using one of five other bases enumerated under art 6 of the GDPR.[26] These have been adapted from the DPD, although EU Member States are now further empowered to introduce additional bases.[27] This is comparable to relying on one of the exceptions to the Consent Obligation under the PDPA.[28]

Most GDPR bases and PDPA exceptions are founded on necessity, and some are even virtually identical. For example, under both regimes, processing that is necessary in the national or public interest is generally lawful,[29] as is processing necessary to protect the data subject's "vital interests" (GDPR),[30] or "life, health or safety [in an emergency]" (PDPA).[31]

Two bases that are unique to the GDPR are of greater interest: (i) processing necessary for contractual performance, and (ii) processing necessary for the controller's or a third party's legitimate interests (balanced against the data subject's reasonable expectations).[32] On their face, they appear to provide generous exceptions to the obligation to obtain consent. Notably, the EU legislator accepts that even processing for direct marketing purposes might qualify.[33] It is submitted that these bases could, possibly inadvertently, operate to mop up the PDPA's 'deemed consent' cases. Using an example from the PDPC,[34] under the PDPA, a data subject who provides her credit card details in exchange for facial treatment could be deemed to have consented to data collection. While consent cannot be deemed under the GDPR, such processing could instead be justified under the banner of being necessary for contractual performance. Either way, lawful processing becomes possible.

---

[26] GDPR, art 6(1)(b)–(f).

[27] GDPR, art 6(2) and rec 40.

[28] PDPA, Second, Third and Fourth Schedules, on collecting, using and disclosing personal data respectively.

[29] GDPR, art 6(1)(e) ("necessary for the performance of a task carried out in the public interest …"); PDPA, paras 1(d) of the Second Schedule, 1(d) of the Third Schedule and 1(e) of the Fourth Schedule ("necessary in the national interest").

[30] GDPR, art 6(1)(d).

[31] PDPA, paras 1(b) of the Second, Third and Fourth Schedule.

[32] GDPR, arts 6(1)(b) and 6(1)(f). See also EU Article 29 Data Protection Working Party, "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" (WP217) (9 April 2014) for specific examples.

[33] GDPR, rec 47.

[34] PDPA Key Concepts at para 12.23.

However, the GDPR's ambit is narrower in one critical way: the fact that personal data is publicly available is *not* in itself a ground for lawful processing. Under the PDPA, data generally available to the public – including that reasonably observable in public spaces – can be processed with few restrictions.[35] The GDPR departs from this in two ways. First, the personal data must be *manifestly* made public *by the data subject*.[36] Second, even where data is manifestly made public, the effect this has is not to legitimise data processing, but only to lift the blanket prohibition on the processing of special categories of data under art 9 of the GDPR.[37] In such circumstances, an additional lawful basis must still be established under art 6. While this second difference could be seen as unnecessarily technical and onerous on controllers,[38] the first is to be celebrated. The requirement is ostensibly borne out of a respect for data subjects' rights; the act of volunteering one's information is a normatively significant exercise of one's autonomy. The mere fact that data is publicly available is not. In fact, where data has been made public against the data subject's wishes, this could well constitute the very antithesis to the data subject's interests.[39]

Will Singapore follow the EU's lead? As it stands under the PDPA, organisations can lawfully use and disclose personal data so long as that data was publicly available for at least an instant in time, even if the individual never intended it for public access and removed it from the public sphere at the earliest opportunity. However, insofar as the PDPA remains an instrument that strives to *balance* data subjects' rights with *organisations'* interests;[40] Europe's data subject-friendly approach is unlikely to gain traction in Singapore. This stems from the PDPC's recognition that,

---

[35] PDPA, s 2(1); PDPA Key Concepts at paras 12.57-12.59. See, for example, *Re SG Vehicles Asia Pte Ltd* [2018] PDP Digest 361.

[36] GDPR, art 9(2)(e).

[37] On 'special categories of data', see GDPR, art 9(1). These categories include data relating to racial or ethnic origin, political opinions, health data, data concerning one's sexual orientation, etc. By contrast, the PDPA does not adopt a bright red line approach. Instead, examples of sensitive data that warrant a higher standard of protection are explored in the PDPC's decisions and advisory guidelines. See, for a summary of these, *Re Aviva Ltd* [2017] SGPDPC 14 at [17]-[18].

[38] There has been suggestion that this would be unnecessary, e.g. Maria Roberta Perugini, " Personal data made public by the 'data subject' and the use of information published on social networks: early observations of GDPR art 9, para 2, letter e" (23 January 2017), *Lexology* (blog), online: <https://www.lexology.com/library/detail.aspx?g=ce9e10b9-de43-4771-9f7b-f52963f7a7b4>.

[39] *Cf.* PDPA Key Concepts at para 12.63. The PDPC's advisory could be construed as evincing some unease with the exception for publicly-available data. The examples raised at para 12.63 all recommend that organisations collecting personal data in public spaces should, as good practice, put members of the public on notice that their personal data may be collected.

[40] *Chesterman* at para 2.49.

were it otherwise, organisations would have to incessantly verify the data's continued public availability, which would be "excessively burdensome".[41]

PURPOSE LIMITATION AND NOTIFICATION

Under the GDPR, a controller must – regardless of its specific *basis* for processing personal data – (i) ensure that processing occurs in a manner compatible with its declared purposes (purpose limitation), and (ii) inform data subjects of these purposes (purpose notification).[42] This is common ground under both regimes, except that the notification obligation does not apply under the PDPA where consent is deemed or where an exception from the Schedule applies.[43] Where consent *is* required, however, the PDPC has routinely stressed that the 'neighbouring obligations' of purpose limitation and notification must be met.[44]

Where purpose limitation is concerned, the GDPR mandates that personal data may only be collected for "specified, explicit and legitimate purposes".[45] Like the PDPA,[46] vague or generic purposes like "improving user experience", "IT-security purposes" and "future research" are unlikely to pass muster.[47] Under both regimes, a flexible and fact-sensitive approach will probably be taken to determine whether a purpose is legitimate (or objectively appropriate under the PDPA[48]), based on parties' reasonable expectations, societal attitudes, etc.[49]

As to the notification obligation, the GDPR sets out relatively more demanding requirements.[50] Controllers are to provide wide-ranging information on their organisations, the data collected (if not already known), the purpose and bases for processing, and any intended data transfers or

---

[41] PDPA Key Concepts at paras 12.60-12.61. See also *Re My Digital Lock Pte Ltd* [2018] SGPDPC 3.

[42] GDPR, art 5(1)(b); *Re AIA Singapore Private Limited* [2016] SGPDPC 10 at [18].

[43] PDPA, ss 18 and 20.

[44] *Re Jump Rope (Singapore)* [2016] SGPDPC 21 at [10]. See also *Re AIA Singapore Private Limited* [2016] SGPDPC 10 at [18].

[45] GDPR, art 5(1)(b).

[46] PDPA Key Concepts at para 14.16.

[47] EU Article 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation" (WP203) (2 April 2013) [WP Opinion on purpose limitation] at 16 and 52.

[48] PDPA, s 18; see also *Re AIA Singapore Private Limited* [2016] SGPDPC 10 at [19]-[20] for an application of this requirement.

[49] WP Opinion on purpose limitation at 19–20.

[50] *Cf.* PDPA, s 20.

recipients,[51] along with storage periods, data subjects' rights, the existence of automated decision-making, and where applicable, the data source.[52]

The GDPR counterbalances these demands by providing for exceptions to the notification obligation. However, these exceptions are not consistently available. Whereas art 14(5) of the GDPR sets out four exceptions (in cases where the data originates from a third-party source), only one exception applies under art 13 (cases where the data originates from the data subject).[53] It is doubtful whether these differences, if deliberate, are justified. As an example, circumstances constituting "disproportionate effort" in an art 14 context are likely to be no less disproportionate or demanding on the controller in an art 13 case.[54] Considerations of fairness and coherence support extending the exception's application to both contexts. One could make the case that it should be the *judge* who then determines whether the *particular* factual matrix crosses the threshold of disproportionality. That being said, EU Member States are empowered to introduce further exceptions pursuant to art 23 of the GDPR, which could leave the final list of exceptions looking quite different.[55]

ACCOUNTABILITY

Relative to its predecessor, the GDPR is decidedly better grounded in the principles of governance and demonstrable accountability.[56] Controllers and processors are expected to take proactive, *ex ante* measures to ensure the lawfulness and integrity of all data processed, as early as when determining the means of processing (i.e. Privacy by Design).[57] Another enshrined principle, Privacy by Default, requires controllers to ensure that, by default, only data *necessary* for their processing purposes are processed.[58] This expectation of data minimisation applies to both the amount of, and access to, data, and the extent and period of their processing retention.[59] Unlike the PDPA, which permits the collection of most data *relevant* to a controller's purposes, only data

[51] GDPR, arts 13(1), and 14(1).
[52] GDPR, arts 13(2) and 14(2).
[53] EU Article 29 Data Protection Working Party, "Guidelines on transparency under Regulation 2016/679" (WP260) (11 April 2018) at paras 56–57.
[54] GDPR, art 14(5).
[55] GDPR, art 23.
[56] GDPR, art 5(2).
[57] GDPR, art 25(1).
[58] GDPR, arts 5(1)(c), 5(1)(e) and 25(2).
[59] GDPR, art 25(2).

that is "adequate, relevant and limited" to these purposes can be collected under the GDPR.[60] Be that as it may, organisations unaffected by the GDPR might still benefit from adopting data minimisation practices, seeing as this might lower the risk of a data breach – a violation under both regimes.[61]

This emphasis on safeguards stems, in part, from a recognition of the consent model's deficiencies. The consent model regards the data subject's consent as the key touchstone of data protection. It presumes, at its heart, the existence of the informed and interested data subject – an idealised construct.[62] In reality, whereas meaningful consent is predicated on carefully-considered choices, the saturation of consent requests and privacy policies today only serve to desensitise data subjects, weakening their ability to respond to such requests.[63] The rise of distributed networks, cloud computing, and the Internet of things has only worsened this predicament by making transactions less discrete and more opaque. Determinations of when and how, or even by whom, our data is processed are thus increasingly difficult to make.[64] An accountability-centric model seeks to resolve these problems by orienting the organisation's interactions – and obligations – to the *regulator*, rather than the disinterested or overwhelmed data subject.

In Singapore, the PDPC has always had this second string to its bow, in the form of the Protection Obligation. Organisations are to protect any data they possess or control using "reasonable security arrangements".[65] Likewise, the GDPR instructs controllers and processors to implement "appropriate technical and organisational measures" to ensure the confidentiality,

---

[60] GDPR, art (5).

[61] Hannah YeeFen Lim, *Data Protection in the Practical Context: Strategies and Techniques* (Singapore: Academy, 2017) at para 5.25.

[62] Policy and Research Group of the Office of the Privacy Commissioner of Canada, "Consent and Privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act" [OPC discussion paper] at 9. See also Gabriela Zanfir, "Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law" in Serge Gutwirth, Ronald Leenes & Paul de Hert, eds, *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (Dordrecht: Springer, 2014) 237.

[63] Bart W Schermer, Bart Custers & Simone van der Hof, "The crisis of consent: how stronger legal protection may lead to weaker consent in data protection" (2014) 16 Ethics and Information Technology 171 at 176-179.

[64] OPC discussion paper at 6.

[65] PDPA, s 24.

availability and security of data.[66] Both regimes also contain provisions on data accuracy[67] and limitations on data storage and retention periods.[68]

Both "reasonable" (PDPA) and "appropriate" (GDPR), in this context, likely involve similar evaluations. Reasonableness in the context of the PDPA considers the nature, form, volume, sensitivity and accessibility of information held, and the potential impact of any unauthorised access, modification or disposal.[69] Indicators like industry practice and software currency are relevant,[70] as are risk levels.[71] Appropriateness in the context of the GDPR considers "the nature, scope, context and purposes of processing as well as the risks … for the rights and freedoms of natural persons".[72] Indicators like adherence to approved codes of conduct and certification under approved mechanisms help demonstrate compliance.[73] What is *distinct* is that appropriateness also factors in the cost of implementing safeguards,[74] tailoring the assessment to the particular organisation's means. It has been suggested that the PDPA lacks such a consideration.[75]

Another difference is that compliance must be *demonstrable* under the GDPR. From obtaining consent[76] to performing internal assessments, organisations are required to document and maintain a record of processing activities,[77] presentable to a supervisory authority on request. While penalties for non-compliance do not appear to include administrative fines, authorities can enforce the obligation using its investigative powers under art 58 of the GDPR,[78] or account for it during sentencing.[79]

---

[66] GDPR, arts 24(1) and 32(1).
[67] PDPA, s 24; GDPR, art 5(1)(d).
[68] PDPA, s 25; GDPR art 5(1)(e).
[69] PDPA Key Concepts at paras 17.2 & 17.4.
[70] *Re K box Entertainment Group Pte Ltd and another* [2016] SGPDPC 1 at [26] and [29].
[71] *Re Metro Pte Ltd* [2016] SGPDPC 7 at [15].
[72] GDPR, art 24(1).
[73] GDPR, arts 24(3) and 32(3).
[74] GDPR, art 32(1).
[75] Foo Ee Yeong Daniel, "Suggestions on the relevance of the Organization's Size to Section 11 of Singapore's Personal Data Protection Act" at section II, online: (2017/2018) 9 *Juris Illuminae* <http://www.singaporelawreview.com/juris-illuminae-entries/2018/suggestions-on-the-relevance-of-the-organizations-size-to-section-11-of-singapores-personal-data-protection-act>.
[76] GDPR, art 7(1) and rec 42.
[77] GDPR, art 30.
[78] GDPR, art 58(1).
[79] GDPR, art 83(2)(f).

The GDPR also elevates the status of Data Protection Impact Assessments [DPIA] from a recommended practice[80] to a mandatory step in some circumstances. Where processing is "likely to result in a high risk", such as where it involves, *inter alia*, evaluations using automated processing, large-scale processing of special data, or large-scale monitoring of public spaces, controllers are to first perform an assessment of the processing's potential impact on data protection.[81] Where such a risk cannot be mitigated, consultations with the supervisory authority should be arranged.[82] One point of interest is art 35(9) of the GDPR, which requires the controller to "seek the views of data subjects … on the intended processing" where appropriate.[83] It is unclear how much weight these opinions will have on supervisory authorities' directions on the scope and permissibility of processing.

Finally, the GDPR mandates the reporting of personal data breaches. Where the integrity of confidentiality of data has been compromised,[84] controllers are bound to notify the relevant supervisory authority of the breach without undue delay.[85] Where the breach is likely to pose a high risk to data subjects, they must too be notified.[86] The PDPA is currently on a convergence path to adopt similar obligations, the PDPC having announced its intention to do so in February 2018.[87]

---

[80] PDPA Key Concepts at para 17.4.

[81] GDPR, art 35. See also EU Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679" (WP248 rev.01) (4 October 2017) at 8-12 on other situations where a DPIA may be warranted.

[82] GDPR, rec 84.

[83] GDPR, art 35(9).

[84] Though not when they are only made temporarily unavailable, e.g. in the event of a power outage.

[85] GDPR, art 33(1). A processor which becomes aware of such a breach is to inform its controller instead: GDPR, art 33(2).

[86] GDPR, art 34(1), though see exceptions under GDPR, art 34(3).

[87] Personal Data Protection Commission Singapore, "Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy" (1 February 2018) at 10–15 (Part III: Mandatory Data Breach Notification). In any case, prompt notification of breaches is already an encouraged practice, and could amount to a mitigating factor in some cases, e.g. in *Re Credit Counselling Singapore* [2017] SGPDPC 18 at [37].

CONCLUSION

While the fundamental tenet of consent is here to stay, the GDPR's broader embrace of accountability is both unmistakable and welcome. In this connection, there is much to be said on the GDPR's treatment of issues like automated decision making and the right to be forgotten. These are exciting developments in a fast-moving area of the law. The impact they will have on future PDPA amendments is certainly a space to watch.