Published on 22 December 2023

LEGAL DUE DILIGENCE IN A DIGITAL AND DATA-DRIVEN ECONOMY

[2023] SAL Prac 27

The transition to a digital and data-driven economy warrants an examination of existing due diligence approaches. As part of the due diligence process, practitioners should take note of recent developments to Singapore's personal data protection landscape and a greater nationwide emphasis on intangible assets, to provide appropriate recommendations and negotiate for the necessary safeguards in a changing environment.

Benjamin **CHEONG**[1]
LLB (University of Leeds);
Advocate and Solicitor (Singapore);
Solicitor, Hong Kong SAR (Non-Practicing);
Senior Accredited Specialist (Data & Digital Economy), Singapore Academy of Law;
Deputy Head, Technology, Media & Telecommunications, Rajah & Tann Singapore LLP.

Keith Kaixian **WONG**[1]
LLB (Hons) (National University of Singapore);
Advocate and Solicitor (Singapore);
Accredited Mediator, Singapore International Mediation Institution;
Associate, Technology, Media & Telecommunications, Rajah & Tann Singapore LLP.

I. Introduction

1 Legal due diligence is integral to mergers and acquisitions ("M&A") and is important to ensure the success of such transactions. However, an evolving digital and data-driven environment requires practitioners to rethink how existing due diligence practices should be tailored to M&A transactions

1 All views expressed in this article are the authors' own.

involving technology companies and/or intangible assets. This is because practitioners need to understand the: (a) unique business models of technology companies; (b) legal issues arising out of creation and commercialisation of intangible assets; and (c) technical issues arising out of the laws on personal data protection and cybersecurity.

2 The increasing focus on technology and intangible assets is evidenced in recent regional and domestic developments. At the Association of Southeast Asian Nations ("ASEAN") level, ASEAN Economic Ministers recently endorsed the study on the ASEAN Digital Economy Framework Agreement ("DEFA"), which includes an assessment on digital trade, cross-border e-commerce, cybersecurity, digital identification ("ID") and digital payments.[2] DEFA allows ASEAN countries to embark on negotiations to undergo digital transformation as a means to spurring economic growth of ASEAN businesses. On the domestic front, Singapore has also positioned itself to become a leading digital economy as part of our smart nation initiatives[3] and recognises data as a "key economic asset in the digital economy".[4]

3 While every legal due diligence has to cover a wide range of issues, this article will focus on the impact of the following areas on legal due diligence:

(a) Singapore's Personal Data Protection Act 2012[5] ("PDPA"); and

(b) the importance of managing intangible assets.

2 "Digital Economy Framework Agreement (DEFA): ASEAN to Leap Forward its Digital Economy and Unlock US$2 Tn by 2030" (19 August 2023) <https://asean.org/asean-defa-study-projects-digital-economy-leap-to-us2tn-by-2030/> (accessed 28 August 2023).

3 "Digital Economy" <https://www.smartnation.gov.sg/about-smart-nation/digital-economy/> (accessed 28 August 2023).

4 Mr S Iswaran, Minister for Communications and Information at Singapore Parl Debates; Vol 95, Sitting No 11; [2 November 2020].

5 2020 Rev Ed.

II. Personal Data Protection Act 2012

4 The PDPA applies to every organisation that collects, uses, discloses, and/or processes personal data in Singapore. Parts 3 to 6A of the PDPA impose certain data protection obligations on organisations,[6] which if not complied with may result in an organisation being in breach of the Act. In any M&A transaction, material data points include employee and customer personal data, and the purchaser's legal practitioners undertaking due diligence must ensure that the collection, use, disclosure and processing of such data points comply with the PDPA, to ensure that the purchaser does not end up with latent liabilities. A McKinsey study of 1,000 individuals found that "the way companies handle consumer data and privacy can become a point of differentiation and even a source of competitive business advantage".[7] This reinforces the importance and value of personal data protection due diligence.

A. Revisions to statutory fines

5 In a digital and data-driven economy, purchasers have pivoted towards technology focused deals such as e-commerce platforms[8] which rely heavily on the collection, use, disclosure and processing of large sets of personal data. Personal data protection due diligence can identify non-compliance and provide pre-emptive recommendations to minimise a purchaser's risk of statutory fines for data protection gaps that may be discovered post-completion.

---

6 Personal Data Protection Act 2012 (2020 Rev Ed) ss 13–17 (Consent Obligation), ss 18 (Purpose Limitation Obligation), ss 21–22A (Access and Correction Obligations), s 23 (Accuracy Obligation), s 24 (Protection Obligation), s 25 (Retention Limitation Obligation), s 26 (Transfer Limitation Obligation), ss 26A–26E (Data Breach Notification Obligation) and ss 11–12 (Accountability Obligation).

7 Venky Anant, Lisa Donchak & James Kaplan & Henning Soller, "The Consumer-Data Opportunity and the Privacy Imperative" (27 April 2020) <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative> (accessed 12 September 2023).

8 "Global C&R M&A Outlook 2022: Asia" <https://kpmg.com/xx/en/home/insights/2022/01/global-consumer-and-retail-m-and-a-outlook-2022-asia.html> (accessed 12 September 2023).

6 From 1 October 2022, the maximum financial penalty which can be imposed on organisations has been revised upwards from a previously fixed sum of S$1m, to 10% of an organisation's annual turnover in Singapore, for organisations with an annual local turnover exceeding S$10m, whichever is higher.[9] Revisions to the statutory fines have raised the financial and reputational risks for purchasers. This enhances the importance of data protection due diligence, prior to consummating any M&A transaction, to identify and remedy gaps and to negotiate and provision for appropriate indemnities and liability caps.

B. Emotional distress

7 In *Reed, Michael v Bellingham, Alex*[10] ("*Bellingham*"), the Singapore Court of Appeal ("SGCA") recognised Parliament's intention to provide robust protection for personal data belonging to individuals[11] and adopted a broader position towards the interpretation of "loss or damage" by including emotional distress as a basis for legal claims. Judith Prakash JCA, in delivering the judgment of the court, clarified that individuals who suffer loss or damage as a direct result of a breach under Pts IV, V or VI of the Personal Data Protection Act[12] have a right of action for relief in civil proceedings in court, but drew the line to clarify that loss of control of personal data does not constitute "loss or damage" as referenced in s 32 of the Personal Data Protection Act.[13] Section 32 of the PDPA referred to in *Bellingham* has since been repealed and is materially reflected in s 480 of the PDPA. Therefore, the SGCA's interpretation of "loss or damage" continues to be of relevance. Section 480(1) of the PDPA provides that:

9 "Amendments to Enforcement Under the Personal Data Protection Act (PDPA) in Updated Advisory Guidelines and Guide" (1 October 2022) <https://www.pdpc.gov.sg/News-and-Events/Announcements/2022/09/Amendments-to-Enforcement-under-the-Personal-Data-Protection-Act-in-updated-Advisory-Guidelines-and-Guide> (accessed 28 August 2023).

10 [2022] 2 SLR 1156.

11 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [98].

12 Act 26 of 2012. As highlighted by the SGCA, for the purposes of this decision, reference was made to the version of the Personal Data Protection Act that was in force in 2018.

13 Act 26 of 2012. *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [108].

> A person who suffers loss or damage directly as a result of a contravention —
>
> > (*a*) by an organisation of any provision of Part 4, 5, 6, 6A or 6B; or
> >
> > (*b*) by a person of any provision of Division 3 of Part 9 or section 48B(1),
>
> has a right of action for relief in civil proceedings in a court.

8 As stated in the judgment, "excluding emotional distress as a head of 'loss or damage' under s 32(1) would cut across Parliament's intention to promote the right of individuals to protect their personal data".[14] However, two limiting principles were espoused, namely:[15]

> (a) The loss or damage must have been suffered directly as a result of a contravention of identified provisions in the PDPA.
>
> (b) Trivial annoyance or negative emotions which form part of the vicissitudes of life will not be actionable.

9 Practitioners should observe the SGCA's multi-factorial framework in ascertaining whether emotional distress constitutes "loss or damage" under s 32(1) of the Personal Data Protection Act[16] (or s 48O(1) of the PDPA). The following non-exhaustive considerations guide the courts in what is ultimately a fact-sensitive inquiry:[17]

> (a) The nature of the personal data involved in the breach, such as financial data and credit ratings. Although not discussed in the judgment, it is observed that the Personal Data Protection (Notification of Data Breaches) Regulations 2021 consider selected financial information about an individual to be information deemed to result in

14 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [77].
15 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [93].
16 Act 26 of 2012. As highlighted by the SGCA, for the purposes of this decision, reference was made to the version of the Personal Data Protection Act that was in force in 2018.
17 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [115].

significant harm to an individual,[18] such that the breach of such information would be considered a notifiable data breach. This includes information such as an individual's net worth,[19] the deposit and withdrawal of moneys by an individual[20] and the creditworthiness of an individual.[21]

(b) The nature of the breach, such as whether the breach of the PDPA was one-off, repeated and/or continuing.

(c) The nature of the defendant's conduct, such as proof of fraudulent or malicious intent.

(d) Risk of future breaches of the PDPA causing emotional distress to the claimant.

(e) Actual impact of the breach on the claimant.

10 Given the broadened scope of "loss or damage" that an individual can claim against an organisation for breaching its data protection obligations, personal data protection due diligence is a necessary tool to pre-empt and mitigate such risks. *Bellingham* highlights the court's preference to uphold a robust personal data protection ecosystem. Consequently, practitioners undertaking data protection due diligence should be cognisant of the wide scope of potential private enforcement claims for "loss or damage" and should: (a) seek confirmation of an organisation's compliance measures with the PDPA (including details of any complaints received from the public in relation to the PDPA) and the personal data protection and privacy practices established by the organisation; and (b) negotiate for the appropriate representations, warranties and indemnities in relation to the parties' rights and liabilities arising out of personal data protection, as may be necessary.

18 Pursuant to s 26B(2)(*a*) of the Personal Data Protection Act 2012 (2020 Rev Ed) and reg 3(1)(*a*) of the Personal Data Protection (Notification of Data Breaches) Regulations 2021.

19 Personal Data Protection (Notification of Data Breaches) Regulations 2021, The Schedule, Pt 1, reg 8.

20 Personal Data Protection (Notification of Data Breaches) Regulations 2021, The Schedule, Pt 1, regs 9–10.

21 Personal Data Protection (Notification of Data Breaches) Regulations 2021, The Schedule, Pt 1, reg 14.

C. SMS Sender ID Registry Regime and the Do-Not-Call regime

11 Following the COVID-19 pandemic, nearly two-thirds of the organisations in a marketing survey reported an increase in the number of marketing channels, with business-to-consumer ("B2C") services reporting a 77% increase.[22] As the PDPA extends to marketing activities, purchasers should conduct due diligence on target organisations that rely heavily on B2C marketing, to ensure that their marketing activities are compliant with the PDPA's SMS Sender ID Registry Regime ("SSIR") and Do-Not-Call regime.

12 The SSIR was set up to protect customers against fraudulent SMS messages that spoof an organisation's SMS sender ID. The SSIR replaces the SMS SenderID Registry pilot led by the Infocomm Media Development Authority and the Monetary Authority of Singapore.[23] From 31 January 2023, SMS messages sent by organisations using alphanumeric sender IDs that have not been registered with the SSIR are labelled "Likely-SCAM". Following about a six-month grace period, messages from non-registered sender IDs are blocked and not delivered to end-users.

13 Where marketing activities are conducted, practitioners conducting legal due diligence should identify and evaluate an organisation's compliance with: (a) the PDPA's Do-Not-Call provisions, which cover voice calls, SMS text messages and fax messages; and (b) the SSIR and any corresponding obligations under the PDPA. This includes confirming with the organisation sending SMS messages to individuals that:

> (a) it has registered with the Full SSIR and paid the annual charge of S$200 for each registered sender ID.

22 Christine Moorman, Jana Soli & Michelle Seals, "How the Pandemic Changed Marketing Channels", *Harvard Business Review* (1 August 2023) <https://hbr.org/2023/08/how-the-pandemic-changed-marketing-channels> (accessed 12 September 2023).

23 Infocomm Media Development Authority, "Full SMS Sender ID Registration is to be required by January 2023", press release (17 October 2022).

(b) it has checked the relevant Do-Not-Call Registry before sending any "specified messages";[24] and

(c) where marketing messages are being sent, the organisation has obtained clear and unambiguous consent from individuals to use their personal data for marketing purposes. Such consent must not be obtained as a condition of providing a product or service.[25] If an individual is deemed to have consented to the sending of a specified message before 2 January 2014 (*eg*, before the Do-Not-Call provisions came into effect), that consent must not have been withdrawn.[26]

14 Early assurance of organisational compliance with the SSIR and the Do-Not-Call provisions can safeguard against unwanted business interruptions and penalties under the PDPA.

D. Use of personal data in artificial intelligence recommendations and decision systems

15 A 2022 global study by International Business Machines Corporation found that 44% of organisations are working to embed artificial intelligence ("AI") into current applications and processes but have not taken steps to ensure AI is trustworthy and responsible.[27] Given the prevalence of AI usage and development, practitioners undertaking legal due diligence should identify an

24 A message is a "specified message" if the purpose of the message, or one of its purposes, is:
(a) advertising, promoting, or offering to supply or provide:
(i) goods or services;
(ii) land or an interest in land;
(iii) business opportunity or an investment opportunity;
(b) advertising or promoting a supplier or provider (or a prospective supplier or provider) of the items listed in sub-paragraphs (i) to (iii) above.
This is adapted from the PDPC's *Advisory Guidelines on the Do Not Call Provisions* (revised 1 February 2021) at para 3.1 <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-on-the-DNC-Provisions-1-Feb-2021.pdf> (accessed 29 November 2023).

25 Personal Data Protection Act 2012 (2020 Rev Ed) s 14(2)(*a*).

26 *Wee Jing Kai Leon* [2023] SGPDPC 8 at [18].

27 IBM Corporation, "IBM Global AI Adoption Index 2022" (May 2022) at p 2.

organisation's use of personal data for such purposes, to evaluate potential risks that a purchaser may be exposed to.

16 The Personal Data Protection Commission launched a public consultation seeking views on the "Proposed Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems" ("AI Guidelines") on 18 July 2023, to clarify how the PDPA applies to the collection and use of personal data by organisations to develop and deploy systems that employ machine learning models to make autonomous decision or assist a human decision-maker through recommendations and predictions.[28]

17 While the AI Guidelines are not legally binding and may be subject to further revisions, they foreshadow the need for compliance with the PDPA where personal data is used for AI-related purposes. As an example, due diligence questionnaires should identify the following issues at an early stage of the due diligence exercise:

(a) categories of personal data collected by the organisation to develop or test the AI system;

(b) whether appropriate consent has been obtained for the use of such personal data to develop or test the AI system;

(c) if the appropriate consent has not been obtained, whether the organisation is relying on any exceptions such as the PDPA's business improvement exception; and

(d) methods to pseudonymise or de-identify the personal data used when designing, training, testing or monitoring AI systems.[29]

28 Personal Data Protection Commission Singapore, *Proposed Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems* (18 July 2023) at para 1.2.

29 Personal Data Protection Commission Singapore, *Proposed Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems* (18 July 2023) at para 7.1.

18 To this end, practitioners conducting due diligence on organisations that develop or integrate AI systems into their products or services, should assess whether the organisations comply with the forthcoming best practices and highlight any shortcomings that may be mitigated by the appropriate pre-completion rectifications, and any representations, warranties and indemnities.

III. Intangible assets

19 Intangible assets ("IA") form more than 90% of the S&P 500 Index's value.[30] On 4 September 2023, the Intellectual Property Office of Singapore launched the Intangibles Disclosure Framework ("IDF") as part of Singapore's IP Strategy 2030,[31] which aims to "provide stakeholders with consistent information about an enterprise's intangibles[32] so that they can make more informed assessments of its business and financial prospects".[33] The IDF is anchored in four pillars: strategy, identification, measurement and management of intangibles. In a digital and data-driven economy, it is imperative that practitioners undertake IA due diligence to identify, measure and evaluate an organisation's management of IA.

A. Founder-developed intellectual property

20 Founders play a key role in developing intellectual property ("IP") materials in an organisation. Successful technology

30 Intellectual Property Office of Singapore, "New Framework for Enterprises to Disclose and Communicate Intangible Assets Launched", press release (4 September 2023) <https://www.ipos.gov.sg/news/updates/ViewDetails/new-framework-for-enterprises-to-disclose-and-communicate-intangible-assets-launched> (accessed 13 September 2023).

31 Intellectual Property Office of Singapore, "New Framework for Enterprises to Disclose and Communicate Intangible Assets Launched", press release (4 September 2023) <https://www.ipos.gov.sg/news/updates/ViewDetails/new-framework-for-enterprises-to-disclose-and-communicate-intangible-assets-launched> (accessed 13 September 2023).

32 The IDF defines "intangibles" as "a non-monetary resource that manifests itself by its economic properties; it does not have physical substance but grants rights and/or economic benefits to its owner".

33 Accounting and Corporate Regulatory Authority & Intellectual Property Office of Singapore, *Intangibles Disclosure Framework 2023* at p 6.

unicorns have, for example, benefitted greatly from the ideas and contributions of their founders. From a due diligence perspective, it is relevant to identify whether the organisation owns the rights to IP developed by the founders. Yet, the lack of formal documentation is commonplace and can raise material concerns for purchasers over ownership rights in such IP.

21 Under Singapore law, the default position under the Patents Act 1994,[34] Copyright Act 2021,[35] and Registered Designs Act 2000[36] of Singapore is that IP created by employees in the course of their employment will vest in the employer. However, the founders of an organisation typically develop material IP *prior* to their formal employment with the organisation. Consequently, due diligence should identify the point at which such IP was created by the founders and require that all rights therein, be assigned to the relevant organisation prior to legal completion. Where IP may have been developed between the founders and other third-party organisations such as universities or research institutions, due diligence should also confirm ownership rights and identify any obligations owed by the founders to such parties.

B. Trade marks

22 Trade marks are used to distinguish an organisation's goods or services and permit the registered mark owner to enjoy a monopoly over its use.[37] As enduring assets that can be renewed[38], sold or licensed, trade marks provide significant long-term commercial value to an organisation. Trade marks also have the potential to be used as collateral for financing.[39] Given the fundamental value of trade marks, due diligence on this class of IA is crucial and should identify issues such as:

34 2020 Rev Ed.
35 2020 Rev Ed.
36 2020 Rev Ed.
37 "Trade Marks" <https://www.ipos.gov.sg/about-ip/trade-marks> (accessed 13 September 2023).
38 In Singapore, registered trade marks are protected for a period of ten years and can be renewed once every ten years.
39 In 2014, the Singapore government trialled a pilot program encouraging selected banks in Singapore to accept trade marks as collateral for loans.

(a) trade marks owned, used or assigned by the organisation;

(b) encumbrances or adverse claims over the trade marks;

(c) validity and renewal of the trade marks in Singapore;

(d) trade mark infringement claims;

(e) licences taken or granted relating to the ownership or use of the trade marks;

(f) marks used by the organisation in the course of their business which have not been registered.

23 For purchasers, the findings from the trade mark due diligence may affect the representations, warranties and indemnities that may be negotiated for, as well as any condition precedents that a vendor may have to undertake. This may also have a bearing on the purchase price. For example, a purchaser may require that trade marks due to expire prior to completion be renewed as a condition precedent, and that the vendor bear the necessary costs of renewal and assignment to the purchaser. The purchaser may also negotiate for an indemnity from the vendor, for actual or pending trade mark infringement claims against the relevant marks.

C. Open-source materials

24 Open-source materials promote public access to the distribution and adoption of software and are ubiquitous in a digital economy. While the licence of open-source material does not typically require any royalty or other fee for its sale,[40] there may be other obligations that are attached to the licence of the material. In this context, due diligence should ascertain what types of open-source licences have been bundled or distributed with the organisation's IP, and the terms and legal obligations of each licence.

40 "The Open Source Definition" (22 February 2023) <https://opensource.org/osd/> (accessed 28 August 2023).

25 For example, the incorporation of copyleft materials into IP rights is a cause for concern, given that an organisation that incorporates copyleft materials into its software may have an obligation to disclose its source codes and other proprietary information in relation to such IP rights to the general public. Failure to do so may constitute a breach of the copyleft licence which could result in certain consequences for the party in breach, such as being required to cease the use of the open-source material.

26 Due diligence should also include a review of source code licences, to determine if all copyright and text redistribution requirements of the open-source licence have been complied with. For example, the open-source MIT Licence[41] requires redistribution of source code to include a prescribed copyright notice, and the full text of the following permission notice in any redistribution of software granted under the licence:

> THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

27 As the use of open-source materials is subject to adherence with all applicable terms of the licence, purchasers looking to acquire or commercialise an organisation's software must obtain confirmation of compliance with such terms and negotiate for the necessary contractual protection mechanisms.

IV. Concluding remarks

28 In a fast changing digital and data-driven economy, practitioners must be cognisant of evolving legal and commercial

41 Open Source Initiative website <https://opensource.org/license/mit/> (accessed 28 August 2023).

issues and take active steps to adapt to existing due diligence approaches. This article has examined the importance of compliance with the PDPA and the value of IA as two areas of focus in this aspect. Where data protection is concerned, practitioners should conduct due diligence bearing in mind:

(a) the impact of non-compliance with the PDPA following the statutory fines increment and potential claims for emotional distress;

(b) the implementation of the SSIR and Do-Not-Call regime; and

(c) the use of personal data in AI recommendations and decision systems.

29 This reflects the fundamental principle of the PDPA which is that:[42]

> … organisations have to be answerable to not just the regulatory authorities, their business partners, but, importantly, to the individuals and their clients and customers whose data is being entrusted to be kept under the control or possession of the organisation or business.

30 Relatedly, parties to a transaction may better reap the benefits of a digital and data-driven economy where identification, measurement and management of IA and compliance with all rights and obligations therein, is done at an early stage of any due diligence exercise.

42 Singapore Parl Debates; Vol 85, Sitting No 75; Col 6; [9 November 2022].