DATA PROTECTION AS PART OF AN ENVIRONMENTAL, SOCIAL AND GOVERNANCE FRAMEWORK*

Amira Nabila BUDIYANO†
LLB (Singapore Management University), Grad Dip (IP and Innovation Management) (Singapore University of Social Sciences);
CIPP/A;
Advocate and Solicitor (Singapore)

Jonathan KAO‡
LLB (Hons) (National University of Singapore);
Advocate and Solicitor (Singapore)

I. Introduction

1 The phrase "Environmental, Social and Governance" ("ESG") appears to be first coined in a report produced for the Asset Management Working Group of the United Nations Environment Protection Finance Initiative and published in October 2005.[1] Consumers and investors have increasingly been using ESG indicators to guide their decision-making, supporting companies and conduct that are sustainable and socially conscious.

2 Customarily, ESG as applied in disclosures and other reporting instruments for an organisation is seen as a segment where organisations discuss their own narrative in other non-financial aspects of the business. It is presented together with other efforts that may not necessarily be profit-making in nature but can reflect well for the organisation's reputation and improve general public perception. Put simply, it makes the organisation more personable. When discussing ESG, different ideas would come to

---

* The views expressed in this article are the authors' personal views and may not be representative of the views of their respective employers.

† Attorney at Kyndryl (Singapore) Pte Ltd.

‡ Counsel, Bird & Bird ATMD LLP, Singapore.

1 Freshfields Bruckhaus Deringer, *A legal framework for the integration of environmental, social and governance issues into institutional investment* (Produced for the Asset Management Working Group of the UNEP Finance Initiative) (October 2005).

mind including corporate social responsibility ("CSR"); environmental awareness and conservation efforts; and workplace inclusion, diversity and balance. There was little structure or consensus on what defines ESG. That is, until more listing bodies started to include the requirement for ESG reporting in listing rules and annual reports, elaborating on some form of standards to adhere to.

3 At the time of writing, there is yet to be a single set of reporting standards for ESG. In 2022, the International Sustainability Standards Board ("ISSB") formally commenced work on developing a baseline for sustainability-related disclosure standards building upon standards by members of the ISSB such as the Global Reporting Initiative ("GRI") and the Sustainability Accounting Standards Board ("SASB"). These standards are expected to give insights into an organisation's resilience through its governance and practices, as well as its exposure to climate-related risks and management of resources. These currently do not include data protection or privacy as an area to be expressly addressed.

4 Nevertheless, the importance of data protection is no longer in doubt with legislation being enacted and revised in all major jurisdictions and ongoing efforts to harmonise obligations across jurisdictions. The collection, processing, storage and sharing of data, personal or otherwise, has been growing exponentially as more services and experiences move online, a trend exacerbated by the COVID-19 pandemic and the push for more "smart" initiatives and proliferation of Internet of Things ("IoT") technologies.

5 So where does data protection or privacy fit into the picture? And is there a more worthy purpose for data protection or privacy to be included within the ESG framework than mere glorification of the organisation? This article seeks to first explore how ESG and personal data protection obligations can intersect. It then explores how data protection or privacy as a standalone component can and should be an integral part within any ESG framework. The authors conclude with several recommendations and proposals on how various bodies can enable this holistic integration. To be clear, this article does not discuss nor makes recommendations as to whether ESG reporting ought to be a mandatory practice in Singapore and much less worldwide. This article is premised on when ESG is indeed reported, to consider inclusion of data protection or privacy items.

II. Intersection with the Environmental, Social and Governance framework

6 Data protection or privacy is not just about compliance with relevant laws and regulations as well as mitigating risks. At its heart across various jurisdictions, it is about recognising the right of individuals to protect their personal data.[2] At the same time, ESG is about accountability to investors, capital market players and consumers about the performance of a company in terms of risks and strategies against certain benchmarking metrics and standards. Therein is the intersection between data protection or privacy and the ESG framework at the very outset: upholding the user or consumer's sovereignty in a capitalistic environment.

A. Environmental

7 The environmental element in ESG broadly focuses on climate-related risks and opportunities. These can include direct and indirect emissions and offsets, resource use and management, pollution and waste, resilience to climate change, risks arising from climate change and opportunities that may arise from climate change.[3]

8 A common theme that perpetuates in data protection obligations or privacy obligations is the need to be clear and precise on the reason for collecting or processing personal data, which is known as "transparency". The principle of frugality in the collection and processing of personal data is also central to privacy or data protection by design. Take not what you do not need, and waste not what you have. Apart from transparency and

2 Under s 3 of the Singapore Personal Data Protection Act 2012 (2020 Rev Ed) ("PDPA"), the purpose of the Act includes the right of individuals to protect their personal data. Whereas under Art 1(2) of the European Union ("EU") General Data Protection Regulation (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) ("GDPR"), it is described that the GDPR protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3 See MSCI ESG Research LLC, *ESG Ratings Methodology* (November 2022).

data minimisation,[4] another closely related principle of data protection by design is "risk minimisation". In the Singapore context, it has been recommended that good practices in the collection of personal data could include collecting the least sensitive types of personal data when different types of personal data are used to achieve the same purpose. Other good practices would be to consider not collecting metadata or removing them if they are not needed, as well as to provide options for users to input selected personal data instead of automatically obtaining it.[5] In turn, "unnecessary personal data" would not be collected by the organisation resulting in no burden of having to protect them, and thereby the organisation is better able to allocate resources effectively.

9 Data protection by design in the General Data Protection Regulation ("GDPR") context speaks about incorporating appropriate technical and organisational measures within an organisation to implement data protection principles in an effective manner and integrate safeguards into processing.[6] A form of certification mechanism can be used to demonstrate compliance.[7] At present, Europrivacy is the only approved certification scheme. What it does is to enable companies to assess and formally certify their data processing compliance for each process. Europrivacy certificates are to be formally recognised in all European Union Member States and will be taken into account by data protection supervisory authorities in case

4 Under the *Guide to Data Protection by Design for ICT Systems* (2019), jointly issued by the Singapore Personal Data Protection Commission ("PDPC") and Hong Kong Privacy Commissioner for Personal Data, data minimisation is defined as to "strictly collect, store and use personal data that is relevant and necessary for the intended purpose for which data is processed".

5 See "Collection of Personal Data by ICT Systems" – Singapore Personal Data Protection Commission and Hong Kong Privacy Commissioner for Personal Data, *Guide to Data Protection by Design for ICT Systems* (2019) at pp 13–14.

6 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, Art 25.

7 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, Art 42(5).

of litigation.[8] A positive benefit for users could potentially be that such certification could help to alleviate concerns as to data protection compliance and dispense with the requirement to conduct full due diligence checks on organisations.

10 Even for the "Environmental" component, we argue that there is not just a strong but also natural intersection between data protection or privacy and ESG in terms of mandating effective resource use and management.

B. Social

11 The social aspect of ESG touches on an organisation's human capital and engagement with the community. This includes health and safety and human capital development, product liability, stakeholder engagement and engagement with society at-large. On the other side, personal data protection or privacy is principally about protecting the interests of individuals and balancing an individual's autonomy over his/her personal data and legitimate business and social interests. The intersection between the two cannot be more obvious. Engagement is key.

12 Data protection or privacy programmes and regimes generally support three concepts. The first is the right of an individual to access, correction and erasure/withdrawal. The second is to enable individuals to engage and exercise these rights by first understanding how that data is used by an organisation and for what end. The third is to hold the organisation accountable to what they have committed themselves to. Employees of an organisation will hold the organisation to these standards, whilst consumers will demand such engagement with the organisation for every transaction.

13 The intersection under the "Social" component is easy to visualise. The intersection for the last component is probably even easier to see.

---

8 Europrivacy, "Press Release: The GDPR European Protection Seal Approved by the EU, a New Era for Privacy and Data Protection Compliance" (12 October 2022) <https://europrivacy.org/en/news/2022-10-14/europrivacy-gdpr-european-data-protection-seal-approved-eu-new-era-privacy-and-data> (accessed 5 March 2023).

C. Governance

14 Governance broadly refers to corporate governance and behaviour, such as the organisation's corporate policies and practices, as well as its conduct. Data protection laws such as the Personal Data Protection Act ("PDPA") and related regulations will dictate the statutory framework for organisations to operate within, but organisations will necessarily have to adopt policies and practices specific to their circumstances to ensure compliance.

15 The Singapore Exchange ("SGX") has come up with a list of core ESG metrics[9] that can be referred to when preparing disclosures to better align between users and reporters of ESG information. Whilst data protection is not yet part of the existing metrics, it can easily fit into three out of the six topics, namely "Certifications", "Alignment with Frameworks" and "Assurance". Legislation already necessitates organisations to have data protection policies and frameworks in place. The Singapore experience also makes local certification, such as the Data Protection Trust Mark, available for organisations to report on the same should they procure them.

16 Another aspect of data protection that enables it to go hand-in-hand with the objective of reporting under "Governance" is the very fact that because of the importance of employee and consumer data to businesses, effective governance of data protection programmes is becoming a board-level responsibility. There are already predictions in various commentaries online of boards assuming responsibility for the performance and success of the organisation's data protection programme and steady adoption of binding corporate rules, and thereby contributing to this component of ESG metrics.

III. Championing data protection or privacy obligations as part of the Environmental, Social and Governance framework

17 It is widely accepted that the "Governance" component is the most likely place where data protection or privacy would reside very well.

9 Singapore Exchange, *Starting with a Common Set of Core ESG Metrics* (December 2021).

However, we propose that data protection or privacy would find a home in every component of any ESG framework.

A. Environmental

18 While not immediately apparent, personal data protection obligations can play a role in an organisation's response to and performance in relation to the Environmental component. The most direct opportunity here is that by promoting data minimisation and reducing data footprint as discussed in the earlier section, there will be a decreasing demand and need for data storage, and the energy required to store data in physical servers at data centres will also decrease.

19 In this section, we discuss what other opportunities there can be under the environmental component. Still with the data centre example, in Singapore alone, the total available data centre capacity was about 1,000Mw across more than 70 operational data centres as of 2021.[10] Accounting for about 7% of electricity consumption in Singapore, there has been a strong push for more efficient data centres with a three-year moratorium that was lifted for pilot applications for data centres that meet stringent efficiency and decarbonisation standards.[11]

20 While the choice of a more efficient data centre would not come within any of the personal data protection obligations, there is the potential for an indirect link from the actual use of data centre capacity and even internal IT systems and equipment. These can extend throughout the life-cycle of the equipment beyond just operations, from production to transport and end-of-life/disposal.

---

10 See Ministry of Trade and Industry, "Written Reply to Parliamentary Question on Data Centres" (11 January 2022) <https://www.mti.gov.sg/Newsroom/Parliamentary-Replies/2022/01/Written-reply-to-PQ-on-data-centres> (accessed 5 March 2023).

11 See Infocomm and Media Development Authority, "EDB and IMDA Launch pilot Data Centre – Call for Application (DC-CFA) to Support Sustainable Growth of DCs" (20 July 2022) <https://www.imda.gov.sg/Content-and-News/Press-Releases-and-Speeches/Press-Releases/2022/Launch-of-pilot-Data-Centre---Call-for-Application-to-support-Sustainable-Growth-of-DCs> (accessed 5 March 2023).

21 We suggest that the Purpose Limitation, Protection and Retention Limitation, and Data Portability obligations can play a key role in an organisation's response to and performance in relation to the Environmental component.

(1) Purpose Limitation, Protection and Retention Limitations

22 The Purpose Limitation obliges organisations to only collect, use or disclose personal data for the purposes that a reasonable person would consider appropriate under the given circumstances and for which the individual has been informed of.[12] On its own, the Purpose Limitation should reduce the personal data collected, used or disclosed by an organisation and the resources required to do so.

23 The Protection and Retention Limitations oblige organisations to take reasonable security arrangements to protect personal data in their possession or under their control, and to cease to retain personal data as soon as the purpose is no longer being served or no longer required for legal or business purposes. Together with the Purpose Limitation these obligations, if judiciously applied, should also reduce the resources required in implementing security arrangements and the need for personal data to be retained or processed.

24 Another area for potential resource efficiencies is in avoiding duplication of efforts in collecting, using or disclosing personal data. The potential for duplication can also come under the Data Portability obligations.

(2) Data Portability

25 The Data Portability obligation is part of the PDPA but will only come into effect when the relevant regulations are issued. Very generally, this obliges organisations to transmit individuals' data in their possession or under their control to another organisation in a machine-readable format.

26 The key intention of the Data Portability obligation was to give individuals greater control over their personal data by enabling their data to

---

12 See Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the PDPA*, para 13.1.

be transmitted between organisations in a commonly used machine-readable format, enabling personal data to be moved across services and enabling greater access to more data by organisations.[13]

27 This has the potential to improve efficiencies and innovation by enabling greater access and transmissibility of personal data but conceptually poses significant risks of duplicating and multiplying datasets across organisations and ultimately their IT resources and service providers.

(3) An opportunity for resource efficiency

28 Taken to a potential logical extreme, the foregoing obligations can be read and applied to enable a common pool of data resources accessible and available to organisations; the assumption being that "at-scale" data resources should be more efficient than having multiple individual resources.

29 Organisations that interface directly with the individuals can already go a long way in fulfilling their Purpose Limitation, Protection and Retention Limitations by engaging the services of trusted service providers. Such service providers are then bound by similar Purpose Limitation, Protection and Retention Limitations in relation to each organisation that engages them, and the data for each organisation should presumably not be co-mingled.

30 By changing the arrangement between organisations and the service providers to one more akin to that of the organisation obtaining data and services from the service provider(s) as a central repository, it is proposed that the service provider(s) should be able to provide better efficiencies in consolidating and deduplicating data resources. The proposed solution would be a cross between data brokers and central identity authorities.

31 A similar approach has been explored in a Practical Guidance issued by the Personal Data Protection Commission ("PDPC") on data collaboration using a common data intermediary. Where data is to be shared between data controllers through the data intermediary the guidance

13 See Personal Data Protection Commission, *Public Consultation On Review Of The Personal Data Protection Act 2012 – Proposed Data Portability And Data Innovation Provisions* (22 May 2019) at para 1.4.

is that, for such sharing to occur, data controllers should establish that an exception to consent applies or otherwise obtain individuals' consent.[14]

32 Having personal data consolidated among a handful of organisations presents significant concerns over data monopoly or oligarchy and most significantly data security. This would somewhat circuitously have to be mitigated by some degree of data segregation potentially by industry and function. More importantly, in order to minimise concerns about monopolies or oligarchies and to establish trust, such service providers should not be privately-held or for-profit but supported by and serving the target individuals and organisations.

33 Government-led examples would be Singapore's "SingPass" and "CorpPass" services that provide a central service for identity verification and personal data retrieval, and "SGFinDex" that provides a centrally-managed system to access and share financial information across different government agencies and financial institutions. Services offered by the industry service providers could be ancillary and pertain to less sensitive personal data.

34 In summary, under the "Environmental" component of any ESG framework, for the reasons discussed above, what may potentially be relevant data protection or privacy metrics could be:

(a) whether energy used for data storage needs is at widely accepted efficient and sustainable levels;

(b) whether data minimisation and transparency as encapsulated under the Purpose Limitation, Protection and Retention Limitations are upheld;

(c) whether data is portable; and

(d) whether data is obtained through resource-efficient means.

B. Social

35 Personal data protection obligations fall neatly within the Social component of ESG as explained above.

---

14 See Personal Data Protection Commission, *Guidance to Data Collaboration Arrangement Involving Common Data Intermediary* (March 2021).

36 Taking the PDPA as a reference point, it is noted that the PDPA obligations are by design primarily intended to protect individuals while providing flexibility for organisations to innovate and conduct business. Compliance with PDPA obligations and responsible use of the bases and additional bases for collection, use and disclosure without consent, as well as exceptions in the PDPA, can promote and be beneficial to society at-large.

37 These include the various bases in the Schedules of the PDPA that allow collection, use and disclosure on the bases of being in the vital interests of individuals, affecting the public or the public interest, legitimate interests (with necessary safeguards and assessments), business asset transactions and business improvement, research purposes and evaluative purposes.

38 The PDPC has also issued various Advisory Guidelines, Guides and Practical Guidance for specific industries and topics including responsible use of biometrics, data collaboration, application to social services, anonymisation and securing of personal data in electronic media just to name a few.

39 The significance of such obligations can be found in the response of consumers to a breach. This can include reputation loss and loss of company value, with certain surveys suggesting that consumers would not do business with a company if there are concerns over data security practices and some 70% would stop doing business with a company if personal data is given away without permission.[15] This has a direct impact on the values of intangible assets such as trade names and marks, and intellectual property.

40 Other instances providing a more concrete illustration of the impact of failure to protect personal data can be seen from record fines imposed on Amazon and Meta for failing to report breaches under the GDPR,[16] the

15 Venky Anant *et al*, "The consumer-data opportunity and the privacy imperative" *McKinsey & Company* (27 April 2020) <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative> (accessed 5 March 2023).

16 Amazon was fined €746m by the Luxembourg National Commission for Data Protection and Meta was fined €405m by the Ireland Data Protection Commission.

lowered sale price in Verizon's acquisition of Yahoo, as well as settlement offers with long-term effects by Equifax.[17]

41 The social demands are clear, and so are the implications of failing to engage as demanded. We therefore propose, under the "Social" component of any ESG framework, the inclusion of minimally the following data protection or privacy metrics:

(a) whether rights of individuals to access, correction, withdrawal/erasure are upheld;
(b) what efforts are being undertaken to further the data security agenda; and
(c) whether incident response policies have been implemented.

C. Governance

42 We argue that the fundamental principle of the PDPA is accountability. This obliges organisations to develop and implement policies, communicate and ensure that such policies are implemented within the organisation, appoint a Data Protection Officer or team to ensure compliance, as well as implement processes and practices to fulfil obligations under the PDPA. As a governance matter, these obligations typically fall upon the directors and key executives to prepare and implement the relevant policies and practices for the organisation, but staff and administrators handling the day-to-day operations are the key in actual and practical compliance.

43 A key focus of recent personal data protection principles is the "by design" approach, where personal data protection principles are considered and incorporated at the time of conceptualising and planning for a system and implemented throughout the life-cycle of the relevant data and system. The "by design" approach requires overall transparency of the relevant system within the organisation so directors, key executives and relevant staff

17 Alejandro Romero, "Brand Exposure: How Exposed Personal Data Impacts Corporate Digital Risk" *Forbes Technology Council* (31 March 2022) <https://www.forbes.com/sites/forbestechcouncil/2022/03/31/brand-exposure-how-exposed-personal-data-impacts-corporate-digital-risk/?sh=1740ba762159> (accessed 5 March 2023).

can be made aware of the potential risks involved and implement the necessary policies and safeguards.

44 Apart from the broader data protection obligations, there is also a push for greater public disclosures and accountability. For example, the US Securities and Exchange Commission has proposed that material cybersecurity incidents are to be disclosed by publicly listed companies, and in Singapore breaches that result in, or are likely to result in, significant harm or are of significant scale must now be reported to the PDPC.

45 Prior to breaches or incidents occurring, pre-emptive measures ought to be taken to minimise the likelihood of such breach or incident, to the extent possible. Data Protection Impact Assessments ("DPIA") or Privacy Impact Assessments ("PIA") would be helpful in this sense. DPIA or PIA are founded upon risk-based assessments of a processing activity, and it is usually up to an organisation to decide if it ought to be conducted. Since this places a lot of autonomy on the organisation with regards to how to check itself, there are other ways that regulations can and have been introduced in order to compel an organisation to remain accountable. For example, in the Philippines, the requirement of mandatory registration of a personal data processing system for a controller or processor that employs 250 persons or more, or those processing sensitive personal information of 1,000 individuals or more, or those processing data that will likely pose a risk to the rights and freedoms of data subjects, was recently introduced with the National Privacy Commission ("NPC").[18]

46 Given the above, there is no greater message on the importance of an organisation's accountability to its consumers and investors in respect of its data protection obligations than if they were taken seriously and driven at board-level. For the "Governance" component of any ESG framework, we propose including at least the following data protection or privacy metrics:

(a) extent of commitment given to data protection programmes and governance of the same;

(b) whether the organisation has data protection policies and frameworks in place and how often they are reviewed;

18 See Republic of the Philippines National Privacy Commission, NPC Circular No. 2022-04 (5 December 2022, effective on 11 January 2023).

(c) whether the organisation has obtained any certification for its processes or what DPIA or PIAs have been done; and

(d) what measures are in place to account to the consumers and public of its data security practices.

IV. Recommendations and conclusion

47 We have discussed at the beginning of this article how ESG and personal data protection obligations intersect at each component. We have made a case for the inclusion of data protection or privacy into any ESG frameworks, as well as proposals for each component. How can we now take the agenda forward to bring data protection as essential reporting items into ESG?

48 Locally, integration can happen at three levels. One is with the support of listing bodies like SGX. As discussed, the core ESG metrics can be expanded to include the points we raised in this article. The second is through an Advisory Guideline, potentially falling under the chapter of Accountability. The third is through industry-led guidelines. For example, for financial institutions, the Monetary Authority of Singapore ("MAS") could include such requirements within its relevant guidelines and circulars for disclosure of sustainability approaches.

49 Beyond Singapore, it can be an uphill task with so many other variables in the picture. However, a good starting point can be a continued revision and update to the ISSB's work, which already holds so much promise, keeping various stakeholders eager for what it can deliver.

50 Nevertheless, what is clear is that although it took almost 20 years for ESG to be a globally accepted concept that is now becoming more uniform and standardised, it will take data protection much less time to be an integral part of it. The time for it will be soon, if not now.