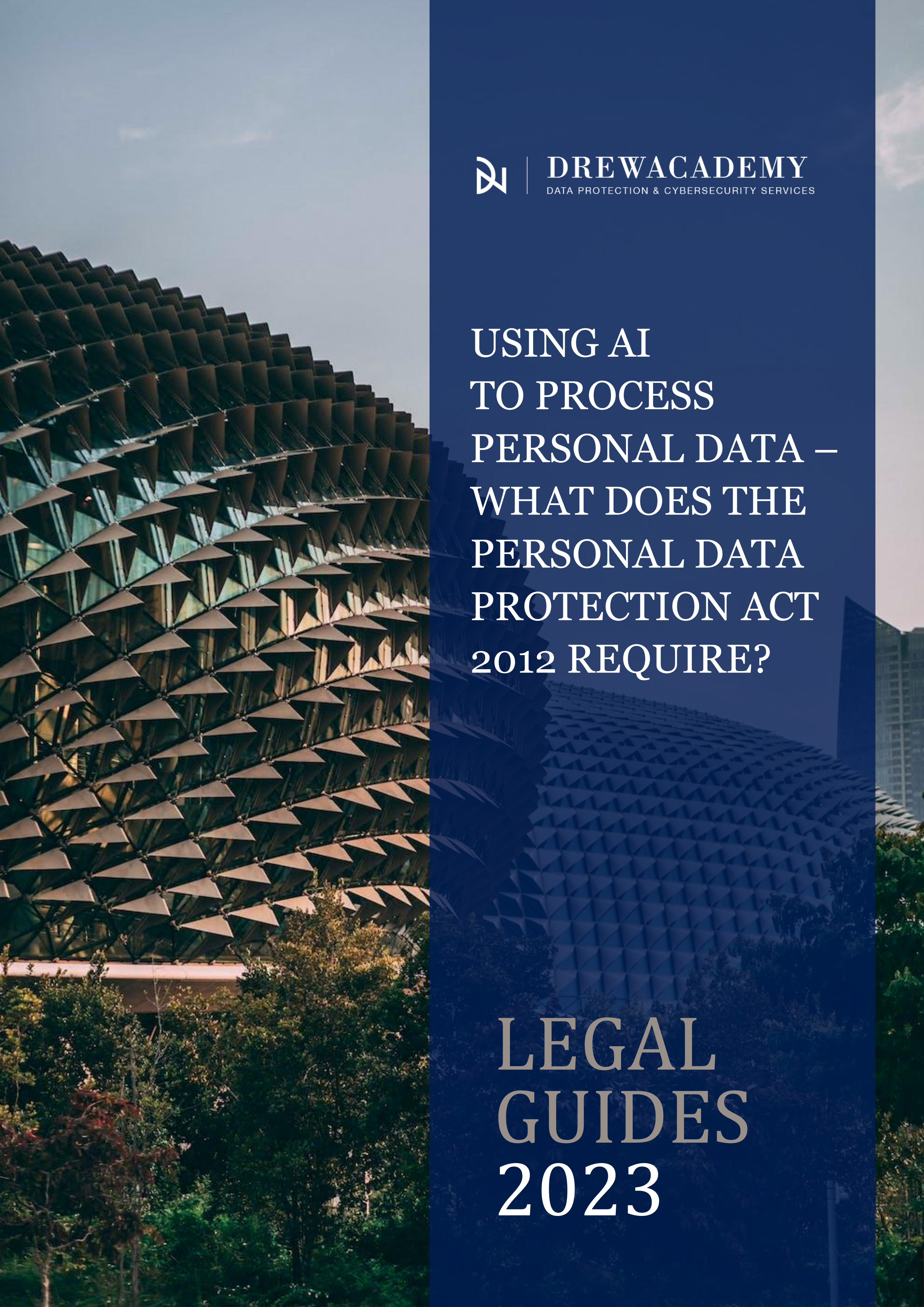

DREWACADEMY
DATA PROTECTION & CYBERSECURITY SERVICES

USING AI TO PROCESS PERSONAL DATA – WHAT DOES THE PERSONAL DATA PROTECTION ACT 2012 REQUIRE?

LEGAL GUIDES 2023

CONTENTS

Developments as of 11 April 2023

USING AI TO PROCESS PERSONAL DATA – WHAT DOES THE PERSONAL DATA PROTECTION ACT 2012 REQUIRE?

Introduction

The Personal Data Protection Act 2012 ("**PDPA**") consists of ten obligations[1] currently in force that organisations need to comply with when collecting, using, or disclosing personal data ("**the PDPA Obligations**"). This article aims to provide a high-level overview of the challenges organisations using artificial intelligence ("**AI**") to process personal data may face in trying to comply with the PDPA:

(a) Part 1 of this article will discuss the PDPA obligations and how the features of AI may affect compliance with the PDPA, together with some ways in which organisations can mitigate the data protection risks associated with using personal data to train an AI model, and when an AI model is deployed to process personal data;

(b) Part 2 of this article will explore the obligations of a "data controller" and a "data intermediary", including whether an organisation may use personal data from another organisation in its possession to enhance its own AI system.

Definitions

In this article, an "AI system" refers to the AI model that has been selected and deployed for use, whereas an "AI model" is created when algorithms (a set of rules/instructions given to a computer for it to do a task) analyse data, leading to an output/result which is examined and the algorithms iterated until the most appropriate model emerges.[2]

"Personal data" is defined under section 2(1) of the PDPA as "*data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access*".

Part 1: The PDPA Obligations

(1) Consent Obligation; (2) Notification Obligation; and (3) Purpose Limitation Obligation

Obtaining consent, and notifying the individual of the purpose for which the data will be used, are all intertwined — these 3 sets of obligations will be addressed together.

Sections 13 to 17 of the PDPA require that an organisation obtain the consent of an individual before collecting, using, or disclosing his personal data for a purpose, unless an exception in the First or Second Schedule to the PDPA applies ("**the Consent Obligation**"). Additionally, for consent to be validly given, the individual must be notified of the purposes for which the organisation is intending to collect, use or disclose their personal data ("**the Notification Obligation**"), where the purposes must be purposes that a reasonable person would consider appropriate in the circumstances ("**the Purpose Limitation Obligation**")[3].

However, organisations that use AI systems may find it challenging to comply with these obligations for the following reasons:

(a) AI systems can be unpredictable and opaque in their operations ("**the black box problem**");
(b) AI systems may apply existing personal data sets for new purposes ("**the repurposed data problem**"); and
(c) for many AI systems, the only way to completely remove an individual's data is to retrain the whole model from scratch on the remaining data ("**the withdrawal of consent problem**").

[1] The PDPA Obligations are as follows: (a) Consent Obligation; (b) Notification Obligation; (c) Purpose Limitation Obligation; (d) Accountability Obligation; (e) Access and Correction Obligations; (f) Accuracy Obligation; (g) Protection Obligation; (h) Data Breach Notification Obligation; (i) Retention Limitation Obligation; and (j) Transfer Limitation Obligation. The 11th obligation, concerning data portability, is not yet in force.

[2] See [3.20] and [3.21] of Singapore's Model Artificial Intelligence Governance Framework.

[3] Section 18 of the PDPA.

(a) The Black Box Problem

Machine Learning ("**ML**") models have seen a rapid increase in popularity over the years. In essence, machine learning is such that through the use of statistical methods, algorithms are trained to make classifications or predictions, and to uncover relationships between data.[4]

However, the type of model used will affect how easily its workings are understood (i.e. whether it is a "black box") — a simple model with easy-to-understand structures and a limited number of parameters (such as linear regression or decision trees) can be understood more easily compared to complex models like Deep Neural Networks with thousands of parameters, although there is no "threshold" for when a model becomes a "black box".[5] "Black box" models are such that even the engineers who design such models (and know the list of the input variables) struggle to understand how the variables are being combined with or related to each other to generate an output.[6] This would mean that it is not always possible to state how the data will be processed and what data (out of all the data collected) is going to be used for the processing.[7]

This may pose a problem when obtaining consent for AI systems to collect, use, and disclose personal data as section 20 of the PDPA requires organisations to inform individuals of the purposes for which their personal data will be collected, used and disclosed in order to obtain their consent ("**the Notification Obligation**"). Due to the opaque manner in which such black box AI systems operate, organisations may not be able to provide information to customers which constitutes sufficient notice under the PDPA.

In this regard, the PDPA does not prescribe a specific manner or form in which an organisation is to inform an individual of the purposes for which it is collecting, using or disclosing the individual's personal data. In order to comply with the Notification Obligation, an organisation should state its purposes at an appropriate level of detail such that an individual is able to determine the reasons and manner in which the organisation will be collecting, using or disclosing his personal data.[8] In particular, an organisation need not specify every activity the AI system will undertake in relation to the personal data when notifying individuals of its purposes. To be transparent, an organisation may specify whether the AI will be making a prediction, recommendation or classification in relation to the data, and whether the output will be subject to review by a human or if the AI system is fully automated.[9]

(b) The Repurposed Data Problem

One of the advantages of using AI is that it can be applied to existing data sets to yield new information and new uses of that personal data. However, organisations must bear in mind the Purpose Limitation Obligation, where the purposes for collecting, using or disclosing the personal data must be what a "reasonable person would consider appropriate in the circumstances"[10].

Organisations should also be alive to the need to obtain fresh consent from individuals if such personal data is being used for a purpose that the individual did not originally consent to at the time their

[4] https://www.ibm.com/topics/machine-learning#:~:text=Machine%20learning%20is%20a%20branch,learn%2C%20gradually%20improving%20its%20accuracy.

[5] https://engineering.dynatrace.com/blog/understanding-black-box-ml-models-with-explainable-ai/

[6] See "*Why Are We Using Black Box Models in AI When We Don't Need To? A Lesson From an Explainable AI Competition*" by *Cynthia Rudin, Joanna Radin, (22 November 2019),* https://hdsr.mitpress.mit.edu/pub/f9kuryi8/release/8

[7] See "*The Law of Artificial Intelligence* ("TLIA")" by Matt Hervey & Matthew Lavy, at 375.

[8] According to the PDPC's Advisory Guidelines on Key Concepts in the PDPA, in determining how specific to be when stating its purposes, organisations may have regard to the following:

- whether the purpose is stated clearly and concisely;
- whether the purpose is required for the provision of products or services (as distinct from optional purposes);
- if the personal data will be disclosed to other organisations, how the organisations should be made known to the individuals;
- whether stating the purpose to a greater degree of specificity would be a help or hindrance to the individual understanding the purpose(s) for which his personal data would be collected, used, or disclosed; and
- what degree of specificity would be appropriate in light of the organisation's business processes.

[9] TLIA at page 366.

[10] See section 3 of the PDPA.

personal data was collected. For example, a social media company makes use of an AI system's facial recognition functions for authentication purposes which users have consented to upon signing-up. The AI system then uses the captured facial data for the purposes of tagging photos of the user uploaded into the social media site. In this scenario, as the new purpose of image tagging is not related to the original purpose of authentication, the social media company would have to obtain fresh consent for its AI system's use of personal data if none of the exemptions set out below apply. Depending on the systems that the organisation has in place, this may be a time-consuming and cost intensive process especially if the organisation has to seek fresh consent from large groups of individuals.

However, an organisation need not obtain fresh consent in the event its AI system repurposes personal data if an exception in the First or Second Schedule to the PDPA applies. For example, Part 5 of the First Schedule and Division 2 of Part 2 of the Second Schedule to the PDPA enable organisations to use personal data that they had collected for another purpose without consent, where the use of the personal data falls within the scope of any of the following business improvement purposes:

(a) Improving, enhancing or developing new goods or services;

(b) Improving, enhancing or developing new methods or processes for business operations in relation to the organisations' goods and services;

(c) Learning or understanding behaviour and preferences of individuals (including groups of individuals segmented by profile); or

(d) Identifying goods or services that may be suitable for individuals (including groups of individuals segmented by profile) or personalising or customising any such goods or services for individuals.

(c) Withdrawal of Consent problem

Under section 16 of the PDPA, individuals may at any time withdraw any consent given or deemed to have been given under the PDPA in respect of the collection, use or disclosure of their personal data for any purpose by an organisation. Organisations must therefore allow an individual who has previously given his consent to the organisation for collection, use or disclosure of his personal data to withdraw such consent by giving reasonable notice.

However, the organisation may face difficulties in ceasing to use the personal data after consent is withdrawn. For one, in respect of many standard ML models, the only way to completely remove personal data used to train the model that the individual no longer consents to is to retrain the whole model from scratch on the remaining data, which is often not computationally and operationally practical[11]. In fact, large scale algorithms can take weeks to retrain and consume large amounts of electricity and other resources in the process. We wish to highlight that the discussion in this section is based on a developing research area – organisations, researchers/academics and regulators are trying to address this issue of whether AI systems (given the way they are trained on data) can 'forget' data that they have been trained on, and this area will continue to evolve.[12]

Some views are that the extent of this problem will depend on the nature of the model. Often, the individual's data would be one of a multitude of examples used to train the model, and the individual's data would not necessarily be stored as-is within the model. Rather, it would be used to determine the "weight" (importance) that the model will give to a particular characteristic to reach an outcome, and once that "weight" is set after training, drawing from thousands of examples, it could be said that the significance of that individual's personal data is that it is only captured as a value within the AI system. Practically, the individual's personal data could then be deleted without affecting the trained model.[13]

[11] See "*Making AI Forget About You: Data Deletion in Machine Learning*"by Antonio A. Ginart, Melody Y. Guan, Gregory Valiant, and James Zou, https://proceedings.neurips.cc/paper/2019/file/cb79f8fa58b91d3af6c9c991f63962d3-Paper.pdf

[12] See "*Humans forget, machines remember: Artificial Intelligence and the Right to Be Forgotten*" by Eduard Fosch Villaronga, Peter Kieseberg, Tiffany Li, available at: http://tiffanyli.com/wp-content/uploads/2018/08/Humans-Forget-Machines-Remember_Final-PDF.pdf

[13] https://www.oreilly.com/radar/how-will-the-gdpr-impact-machine-learning/

Furthermore, if consent is withdrawn, all data processing operations that were based on consent and took place before the withdrawal of consent remain lawful — it is just that going forward, the data processing actions must cease.[14] Therefore, the withdrawal of consent does not equate to needing to delete the personal data used to train the model in the past.

On the flip side, there are some types of models (e.g. Support Vector Machines) that will retain within the model some key individual examples from the training data to help it distinguish between new examples when it is deployed.[15] Depending on how the model is designed, there might be a built-in function to easily retrieve these stored examples and delete them so that they do not continue to be used.[16]

Nevertheless, in the event that an individual rescinds his consent to the collection, use and disclosure of personal data by an AI system, the organisation can continue to make use of that data set without the individual's consent if an exception in the First or Second Schedule to the PDPA applies.

(4) Accountability Obligation

Under sections 11 and 12 of the PDPA, organisations must undertake measures to ensure that they can meet their obligations under the PPDA. For example, an organisation must develop and implement data protection policies and practices, and ensure that its staff are aware of such policies and practices.

Presently, the PDPA does not prescribe any specific accountability obligations in relation to the use of AI systems to process personal data. Unlike the European Union's General Data Protection Regulation, the PDPA does not contain a right for individuals not to be subject to a decision solely based on automated processing ("ADM"), and if the individual is subject to such ADM, that the individual will be given meaningful information about the logic involved in the system as well as the significance and envisaged consequences of such processing for the individual, and have the right to obtain human intervention and also to contest the decision.

But this does not mean that organisations need not be accountable to their customers in relation to how their AI system is collecting, using, or disclosing their customers' personal data. It is always in the best interests of organisations to develop and implement policies and practices for the safe, ethical and transparent use of AI as it enhances consumer trust.

In this regard, it would be helpful for organisations to refer to the Model Artificial Intelligence Governance Framework ("**Model AI Governance Framework**") issued by the Personal Data Protection Commission. The Model AI Governance Framework[17] provides detailed and readily implementable guidance to private sector organisations to address key ethical and governance issues when deploying AI solutions. Such guidance may even help organisations overcome some of the PDPA-specific challenges that they face when using AI systems. For instance, to overcome **the Black Box problem** (discussed above), the Model AI Governance Framework recommends[18] organisations to, amongst others, incorporate descriptions of the AI solution's design and expected behaviour into product or service descriptions and system technical specifications documents (e.g., including design decisions in relation to why certain features, attributes or models are selected in place of others). This helps provide

[14] https://iapp.org/media/pdf/resource_center/wp29_consent-12-12-17.pdf. See also 12.52 of the PDPC's Advisory Guidelines on Key Concepts in the PDPA.
[15] https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/how-do-we-ensure-individual-rights-in-our-ai-systems/
[16] https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/how-do-we-ensure-individual-rights-in-our-ai-systems/
[17] Please see our article on "Issues you must consider before deploying artificial intelligence in your business: an explainer of Singapore's Model Artificial Intelligence Governance Framework", available at: https://www.drewnapier.com/DrewNapier/media/DrewNapier/Incorporating-Singapore-Model-Artificial-Intelligence-Governance-Framework-into-your-business.pdf.
[18] See page 44 of the Model AI Governance Framework.

greater clarity on an AI model to customers by giving understandable and digestible insights into how the model operates.

Apart from the general obligation to be accountable, the PDPA also requires specific measures to be implemented. Section 11(3) of the PDPA requires an organisation to designate one or more individuals to be the Data Protection Officer ("**DPO**"). The DPO is responsible for ensuring that the organisation complies with the PDPA. For the DPO of an organisation that makes use of AI systems, a very real and live issue is how much knowledge the DPO must have of the AI system and how it operates for the DPO to effectively execute his duties and ensure that the organisation is PDPA-compliant.

(5) Accuracy Obligation

Section 23 of the PDPA requires an organisation to make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete if the personal data is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates.

Organisations that utilise AI solutions to make automated decisions that can impact their customers have to be mindful of the accuracy of the personal data upon which the decisions are based on. For instance, insurance companies that use AI to determine the premiums for each individual must ensure that the AI is using up-to-date personal information when making its decision.

(6) Access Obligation

Under section 21 of the PDPA, individuals have the right to request for access to their personal data that is in the possession or under the control of an organisation. When an access request is made by an individual, the organisation must, unless an exception applies, as soon as reasonably possible provide the individual with information about their ways in which his personal data has been or may have been used or disclosed by the organisation within a year before the date of the request.

Organisations that develop their own AI systems may face issues complying with the Access Obligation. Specifically, organisations may face difficulty trying to identify the individual's data in their training dataset, because identifiers such as names and contact details may have been stripped, although there may still be sufficient unique identifiers in that data for it to be used to identify the individual it relates to, whether on its own or in combination with other data the organisation has.[19] This means that if the individual makes an access request, the organisation may not be able to comply with such request if they are unable to link the data used to the individual.

On this note, the PDPA does stipulate[20] that an organisation need not comply with an access request "if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests". Given that linking personal data to specific individuals can sometimes be a difficult process due to the sheer volume of training data involved, the organisation may be able to justify its non-compliance with the access request if the time and costs involved are unreasonably prohibitive.

(7) Correction and Data Retention Obligations

Section 22(1) of the PDPA provides that an individual may request an organisation to correct an error or omission in the individual's personal data that is in the possession or under the control of the organisation ("**the Correction Obligation**").

[19] See "*How do we ensure individual rights in our AI systems*" by Information Commissioner's Office*,* https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/how-do-we-ensure-individual-rights-in-our-ai-systems/

[20] Please refer to paragraph 1(*j*) of the Fifth Schedule to the PDPA.

Under Section 25 of the PDPA, an organisation must cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data, and retention is no longer necessary for legal or business purposes (“**the Retention Limitation Obligation**”).

Similar to the problems associated with the Withdrawal of Consent, organisations may not be able to comply with the Correction and Retention Limitation Obligations without re-training the model (either with the corrected data, or without the deleted data), or deleting the model altogether. This is often a costly and laborious exercise. However, if the request for correction relates to the model’s output or the personal data that is going to be input into the model to obtain an output — such that it is not a request for correction of the training data that the model has previously been trained on — this is something that an organisation can more easily accede to.

Nevertheless, the Retention Limitation Obligation does not prevent organisations from retaining personal data if it is necessary for a legal or business purpose. In the Advisory Guidelines on Key Concepts in the PDPA, the PDPC has recognised the following situations as likely being necessary for a business purpose:

(a) the personal data is required for an organisation to carry out its business operations, such as to generate annual reports, or performance forecasts; or
(b) the personal data is used for an organisation’s business improvement purposes such as improving, enhancing or developing goods or services, or learning about and understanding the behaviour and preferences of its customers.

For example, if an e-commerce company is using an AI model to learn about its customers’ preferences, the company can continue to retain the personal data collected by the AI model so long as the data is being used for business improvement purposes.

It may also be plausible for the organisation to justify retaining the data that the system was trained on so that it may review why the AI system made a decision in a particular manner, in the event of a challenge from affected individual, or pursuant to regulatory requirements, or to defend against liability.

Similarly, an organisation does not need to comply with a correction request from an individual if the organisation is satisfied on reasonable grounds that the correction should not be made (section 22(2) of the PDPA) or if any of the exceptions under the Sixth Schedule to the PDPA apply (e.g. the data is derived personal data).

(8) Transfer Limitation Obligation

Developers, vendors, and end-users of an AI system are not always located in one country. Furthermore, programming code, training datasets and predictive outcomes are increasingly held in disparate locations all around the world[21]. As such, organisations should be aware of cross-border flows of personal data when developing or using AI systems. For instance, datasets collected in Singapore may be transferred overseas for use in training and developing an AI system overseas.

Under the PDPA, an organisation must ensure that any overseas transfer of personal data is in accordance with the requirements prescribed under the Personal Data Protection Regulations 2021 (“**PDPR**”). In brief, an organisation may transfer personal data overseas if it has taken appropriate steps to ensure that the overseas recipient is bound by legally enforceable obligations or specified certifications to provide the transferred personal data a standard of protection that is comparable to that under the PDPA.

[21] See “*AI Ethics in Cross Border Commerce*” by UNECE, https://unece.org/fileadmin/DAM/cefact/cf_forums/2020_October_Geneva/PPTs/AI_SAgarwal-AI-EthicsCrossBorderCommerce.pdf

(9) Protection Obligation; and (10) Data Breach Notification Obligation

Section 24 of the PDPA requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control ("**the Protection Obligation**").

When using AI systems, organisations may open themselves up to new vulnerabilities. These vulnerabilities may make it easier for cybercriminals to penetrate into the organisations' systems and cause significant damage. For example, model-inversion attacks have demonstrated the capability of adversaries to extract user information from trained ML models. Organisations should therefore be proactive and aim to develop a robust and resilient info-comm technology system (ICT) to protect against data breaches. In this regard, organisations can refer to the PDPC's Guide to Data Protection Practices for ICT Systems which compiles best practices that should be adopted by organisations in their ICT policies, systems and processes to safeguard the personal data under their care.

In the event of a data breach, organisations should note that Part 6A of the PDPA sets out requirements for organisations to assess whether a data breach is notifiable, and to notify the affected individuals and/or the PDPC where it is assessed to be notifiable ("**the Data Breach Notification Obligation**").

Part 2: Am I a "data intermediary" or a "data controller"? Can I use personal data from another organisation in my possession to enhance my own AI system?

The PDPA draws a distinction between organisations that collect data for their own purposes (referred to as a "Data Controller") and an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation (referred to as a "Data Intermediary"). Unlike a Data Controller which is subject to all of the PDPA obligations, a Data Intermediary will only be subject to the following PDPA obligations: (a) the Protection Obligation; (b) Retention Limitation Obligation; and (c) Data Breach Notification Obligation.

Whether an organisation is a Data Intermediary or Data Controller depends on what activities it undertakes. Organisations should bear in mind that even if they are a Data Intermediary, if they use or disclose personal data in their possession beyond the remit granted by the Data Controller (i.e. an organisation "exercised its own judgment in determining the purpose and manner of such use and disclosure of the personal data"[22]), they will be responsible for complying with all the data protection obligations under the PDPA.[23] Furthermore, an organisation may act in both roles for different types of processing activities – it could be a Data Intermediary vis a vis Company A, but a Data Controller in relation to its own internal processing activities.

Another issue that will become more relevant with the increasing use of AI is whether an organisation (Organisation A) that processes personal data for another organisation (Organisation B) using Organisation A's AI system may use the data from Organisation B to improve the accuracy and functioning of its own AI system. There is no regulatory guidance as yet from Singapore. The French data protection authorities have issued guidance in January 2022 (only available in French) on when organisations may do so, stating that the data controller must expressly authorise the data processer ("data intermediary" using Singapore's terminology) in writing to reuse the personal data for its own purpose, and only if certain conditions are fulfilled, namely (1) if the processing is not based on the consent of the data subject or under EU/member state law, the data controller must determine whether this further processing is compatible with the purpose for which the data was originally collected; (2) the initial controller must inform the data subjects of the new purpose for which the data is being used.[24] The processor will then become the controller of the subsequent processing.

[22] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-17-May-2022.pdf at [6.25]
[23] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Managing-Data-Intermediaries--2020.pdf at page 7
[24] https://www.dataguidance.com/news/france-cnil-stipulates-conditions-processor-reuse-data

In this regard, it is very important that an organisation that develops AI systems for other organisations is clear as to its rights and obligations vis-vis the other organisations when it processes personal data obtained from them. Such organisations should consider including provisions in their written contracts to clearly set out each organisation’s responsibilities and liabilities in relation to the personal data in question.[25]

Conclusion

With the use of AI becoming commonplace in society, organisations must still be cautious. As much as AI can enhance the relationship between customers and organisations by offering more personalised services, improving service quality, and enhancing the speed at which such services are offered, it can also lead to a breakdown in trust if organisations are found to be misusing and misappropriating personal data when using such AI systems. The protection of data should always remain the cornerstone of organisations, especially in this age where many consumers are becoming more conscious of the ways in which their personal data is being used.

Drew Academy wishes to acknowledge our Associate Shaktivel Arumugam for assisting in the preparation of this article.

The content of this article does not constitute legal advice and should not be relied on as such. Specific advice should be sought about your specific circumstances.

[25] See 6.24 of PDPC’s Advisory Guidelines on Key Concepts in the PDPA

DREW DATA PROTECTION & CYBERSECURITY ACADEMY

Drew Data Protection & Cybersecurity Academy (Drew Academy) was established in 2020 by Drew & Napier to help our clients build their capabilities and develop and implement organisational strategies, structures, policies and processes to meet their legal, regulatory and compliance obligations. Drew Academy offers a range of courses in areas such as data protection, cybersecurity, data governance and in-house commercial practice. A particular focus for us is the delivery of workplace learning solutions and development of customised training courses. We also offer outsourced DPO services and data protection consulting services through our experienced team of practitioners.

Drew Academy is helmed by Lim Chong Kin and David N. Alfred. Our course leaders are experienced in various aspects of data and cyber governance, data protection, cybersecurity engineering and in-house commercial practice.

ARTIFICIAL INTELLIGENCE AND DIGITAL TRUST

Drew & Napier's Artificial Intelligence (AI) and Digital Trust practice brings together its expertise across several technology-related domains and in fields as diverse as data protection, cybersecurity, healthcare, Fintech, intellectual property and competition law (to name a few) to advise clients on the full range of legal issues relating to AI and Digital Trust. In addition to advising on commercial, regulatory and international / cross-border issues, our advice extends into areas such as governance and ethics as we seek to enable our clients to navigate areas where laws and legal principles are still emerging.

Working together with the Drew Academy, we provide solutions that reflect our deep understanding of underlying technologies, the risks and uncertainties involved and practical business considerations. Internationally, there is a growing consensus on AI governance.

For more information on our experience, please contact:

Lim Chong Kin
Managing Director, Corporate & Finance;
Co-Head, Data Protection,
Privacy & Cybersecurity Practice;
Co-Head, Drew Data Protection &
Cybersecurity Academy

T: +65 6531 4110
E: chongkin.lim@drewnapier.com

David N. Alfred
Director, Corporate & Finance;
Co-Head, Data Protection,
Privacy & Cybersecurity Practice;
Co-Head and Programme Director,
Drew Data Protection &
Cybersecurity Academy

T: +65 6531 2342
E: david.alfred@drewnapier.com

Anastasia Su-Anne Chen
Director, Corporate & Finance

T: +65 6531 4123
E: anastasia.chen@drewnapier.com

Cheryl Seah
Director, Corporate & Finance

T: +65 6531 4167
E: cheryl.seah@drewnapier.com

DREWACADEMY
DATA PROTECTION & CYBERSECURITY SERVICES

10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

www.drewnapier.com/Academy

T: +65 6531 4152
F: +65 6535 4864
E: academy@drewnapier.com

In association with

DREW & NAPIER