PERSONAL DATA PROTECTION COMMISSION

[2025] SGPDPC 6

Case No. DP-2310-C1622

In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012

And

Marina Bay Sands Pte. Ltd.

… *Organisation*

DECISION

Marina Bay Sands Pte. Ltd.

Lew Chuen Hong, Commissioner — Case No. DP-2310-C1622

28 October 2025

Introduction

1 On 25 October 2023, the Personal Data Protection Commission (the "**Commission**") received a notification from Marina Bay Sands Pte. Ltd. (the "**Organisation**") about a data breach incident (the "**Incident**") whereby a threat actor had used the account credentials of six (6) existing Sands Rewards Lifestyle ("**SRL**") members to access the customer records of approximately 665,495 SRL members (the "**Affected Data**"). Investigations later revealed that the Affected Data was exfiltrated and made available for sale online on the dark web.

2 The Commission commenced investigations to determine whether the circumstances relating to the Incident disclosed any breaches of the Personal Data Protection Act 2012 ("**PDPA**").

3 On 6 May 2024, the Organisation requested for the investigation to proceed under the Expedited Decision Procedure, which the Commission acceded to. To this

end, the Organisation voluntarily and unequivocally admitted to the facts set out in this decision, and to the Organisation's breach of section 24 of the PDPA.

Facts of the Case

4 The Organisation is an integrated resort which operates amongst other things, a hotel, casino, shopping mall and the ArtScience Museum. The Organisation also offers, amongst others, the following two membership programmes:

(a) **SRL** – enables members to earn points through spending on at various attractions operated by the Organisation, which can then be redeemed for rewards such as discounts and vouchers.

(b) **ArtScience Friends** ("**ASF**") – Existing SRL members that are visitors of the ArtScience Museum have the option to also join the ASF membership programme to access additional benefits and privileges relating to the ArtScience Museum such as priority entry and discounts at the ArtScience Museum's retail stores.

Security measures relating to SRL and ASF members' data

5 As part of the SRL and ASF membership programmes, the Organisation collected the personal data of approximately 1.9 million individuals, including their names, email addresses, phone numbers, countries of residence, membership information among other types of personal data.

6 To balance the twin imperatives of protecting data relating to both SRL and ASF membership programmes and creating a smooth customer experience for members, prior to the Incident, the Organisation enacted a policy of segregated and differentiated access controls for different types of data:

(a) Members could access both the SRL and ASF webpages from the Organisation's website and ArtScience Museum website respectively, through a 4-digit Personal Identification Number ("**PIN**"), with the initial PIN set by default based on individual members' birthdates. This is subject to an automatic lockout in the event of 5 failed login attempts within a 24-hour window (the "**Password Policy**"). This allowed members to access basic identification, contact information and membership tier.

(b) To obtain access to additional data such as “Account Information”, “Dollars History”, “Vehicle Registration” and “Transaction History”, members were required to complete an SMS or email one-time password (“**OTP**”) verification with CAPTCHA. OTP verification is required for each user session.

(c) To ensure that members are only able to carry out activities related to their own accounts on the Organisation’s website, it also implemented an access token verification policy (“**Token Verification Policy**”), where an access token is generated for a 30-minute window after a user successfully logged into one of its webpages. When a user made a Hypertext Transfer Protocol (“**HTTP**”) request to the ASF web server to access a part of the Organisation’s network, a token verification check was carried out to authenticate that the request was related to the same user ID as the access token. If the check was unsuccessful, users would not be granted permission to carry out the requested activity.

(d) To earn and redeem loyalty points to benefit from the privileges of membership, SRL / ASF members were required to be physically present at the Organisation’s property and to present their membership card.

7 Prior to the Incident, the Organisation also:

(a) Implemented a set of data protection and security policies, guidelines, standards and procedures, including the following:

i. Personal Data Protection Policy Manual;

ii. Data Retention and Classification Policy;

iii. IT Acceptable Use Policy;

iv. Information Security Program Policy;

v. IT Software Asset Management Standard;

vi. Cyber Security Monitoring Standard;

vii. Enterprise Cyber Incident Response Plan;

viii. Tactical Incident Response Plan;

ix. Malware Protection and Vulnerability Management Standard;

(b) Employed security monitoring tools;

(c) Put in place a Security Operations Centre to monitor, prevent, detect and assist in investigating and responding to cyber threats;

(d) Performed regular software security patching;

(e) Carried out regular vulnerability assessment scans, architecture reviews, threat risk assessments, code scans, code reviews and penetration testing;

(f) Conducted regular audits across IT systems to ensure the effectiveness of security controls;

(g) Obtained certifications for the ISO/IEC 27001[1] and the PCI DSS[2] standards; and

(h) Conducted data protection and security training sessions amongst the Organisation's staff.

The Incident

8 From 19 to 20 October 2023, an unknown threat actor circumvented the Organisation's security arrangements to access and exfiltrate the Affected Data.

[1] An international standard to manage information security jointly published by the International Organization for Standardization and the International Electrotechnical Commission.
[2] Payment Card Industry Data Security Standard.

Initial Access to the Compromised Accounts

9 The threat actor initially gained unauthorised access to six (6) ASF accounts (the "**Compromised Accounts**") through "password spraying" whereby the same password was used on many SRL and ASF accounts until access was obtained. By virtue of the Password Policy, all the default SRL / ASF account passwords were 4-digit PINs based on the birthdates of the individual members, which made the password spray method effective.

10 Thereafter, the threat actor used the 6 Compromised Accounts to make various successful HTTP requests from the ASF webpage to access the personal data of other SRL members. This enabled the threat actor to use the Compromised Accounts as a springboard to access the data of other SRL members identified at [18] below, which was anomalous for two reasons:

(a) As explained in [6(a) to (c)], access to the Compromised Accounts should have only allowed the threat actor to access the six individual members' basic identification, contact information and membership tier, and not the personal data of other SRL members.

(b) The Token Verification Policy should have only allowed the Compromised Accounts to make HTTP requests relating to their own user IDs, and not the user IDs of other SRL members.

The Misconfiguration Error

11 Investigations revealed that the above anomaly stemmed from a misconfiguration error during the Organisation's migration to a new middleware software platform[3] between September 2022 and March 2023 (the "**Migration Exercise**"). The Migration Exercise involved, amongst other things, the wholesale replication of the Application Programming Interface ("**API**") configurations previously contained in the old middleware platform onto the new middleware platform (the "**API Replication**"). Significantly, the Organisation opted to effect the API Replication process manually.

12 The employee in charge of the API Replication ("**Employee**") was tasked to manually collate a list of all the APIs and their respective calling app IDs[4] into an inventory list for the purpose of the API Replication ("**Inventory Listing**"). However,

[3] Middleware refers to the software that lies between an operating system and the applications running it, and functions as a hidden translation layer to enable communications and data management for distributed applications.

[4] An identifier associated with a specific application that is used to, amongst other things, ensure that any calls or messages made by an application are legitimate and authorised.

the Employee inadvertently omitted the external ArtScienceMuseum calling app ID from the Inventory Listing. Consequently, as the Inventory Listing was subsequently utilised to configure the token check configuration in the new middleware platform, the Token Verification Policy did not apply to the ASF webpage (the "**Misconfiguration Error**").

Access and exfiltration of the Affected Data

13 The Misconfiguration Error created an acute security vulnerability by enabling anyone accessing the ASF webpage with a valid access token to manipulate the parameters of the member ID (which was in a guessable numeric format) in the HTTP request to access the personal data of any other SRL members via a HTTP request.

14 The threat actor exploited this vulnerability to gain unauthorised access to the personal data of 665,495 SRL members (i.e. the Affected Data) comprising the following categories of personal data:

Type of Personal Data	**Number of Affected Individuals**
Names	663,703
Email Addresses	487,639
Phone numbers	663,703
Countries of Residence	496,393
SRL membership numbers and tiers	665,495

15 Subsequently, the Organisation confirmed to the Commission that the Affected Data was put up for sale on the dark web, evidencing that the Affected Data was exfiltrated by the threat actor.

Remedial actions

16 Following discovery of the Incident, the Organisation implemented the following remedial measures on the day itself, and within three months:

Actions to mitigate the effects of the Incident

(a) Deactivated the Compromised Accounts;

(b) Enabled the Token Verification Policy for the ASF webpage, and conducted penetration testing to verify that this was effective to deny access token reuse on the ASF website;

(c) Inspected and validated all the rest of the Organisation's webpages to ensure that the Token Verification Policy was enabled;

(d) Notified the affected individuals;

Actions to prevent recurrence of the Incident or similar incidents

(e) Enhanced the Token Verification Policy to mandate and automate application checks for all of the Organisation's webpages;

(f) Enhanced the Organisation's software configuration testing process to revalidate the Token Verification Policy for all of the Organisation's webpages prior to going live;

(g) Enhanced security monitoring by developing and implementing a script to detect and alert access tokens used to request for multiple customer records;

(h) Setting up digital accounts for all SRL members with different usernames and passwords (with a higher level of complexity) for members to access their membership via any digital platforms; and

(i) Restricted the use of 4-digit pins with physical membership cards to only on-premises transactions.

Findings and Basis for Determination

Whether the Organisation contravened the Protection Obligation under section 24 of the PDPA

17 Based on the circumstances of the Incident as set out above, the Commission's investigation focused on whether the Organisation had breached its obligation under section 24 of the PDPA to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the "**Protection Obligation**"). Given the high volume of personal data in the Organisation's possession, the Organisation is obligated to implement security arrangements that were commensurate with its higher-level security needs to discharge the Protection Obligation.

Misconfiguration Error

18 The Commission has consistently held that organisations cannot rely solely on their employees performing their duties properly as a security arrangement to protect personal data, and that organisations must also put in place processes to ensure that

any step(s) required from employees are properly taken[5]. Where the employees' actions may affect personal data of higher volumes and/or sensitivity, and where such actions involve a higher susceptibility to human error, more robust processes should be implemented. The Commission had previously opined in its Guide to Data Protection Practices for ICT Systems ("**ICT Guide**") that when implementing ICT security measures, organisations should as a **basic practice** do the following:

> "**Automate build and deployment processes to minimise manual steps and hence reduce human errors**. For example, execute predefined scripts instead of manually typing out commands each time a new build of an application is required; this **eliminates errors in typing and the possibility of accidentally leaving out certain commands**, as well as in deploying the new build to the wrong environment, such as deploying a test build to the production environment."
>
> (emphasis added)

19 In the present case, the Migration Exercise exposed a large volume of personal data in the Organisation's possession to data protection risks. Additionally, the manual nature of the API Replication meant that more robust processes were required to mitigate the risks of human error. In this regard, the Commission highlighted in the ICT

[5] *Re E-Commerce Enablers Pte Ltd* [2023] SGPDPC 6 at [17-18]. See also *Re Furnituremart.sg* [2017] at [21], *Re DataPost Pte Ltd* [2017] SGPDPC 10 at [11] and *Re Aviva Ltd* [2017] SGPDPC 14 at [28-30].

Guide that processes such as automation are meant to address risks associated with human error, such as accidentally leaving out of certain commands when a new application is being built and deployed.

20 Instead, the Organisation relied entirely on the Employee to carry out the API Replication manually. This design flaw heightened the susceptibility of the API Replication to human error, which eventuated in the form of the Misconfiguration Error. This engendered a vulnerability in the Organisation's system that was exploited by the threat actor to access and exfiltrate the Affected Data.

21 In relation to the Employee responsible for the Misconfiguration Error, the Organisation submitted to the Commission that:

(a) Due to the Employee's expertise in middleware applications and consistent high performance, the Organisation was confident of the Employee's ability to lead the Migration Exercise; and

(b) The Employee had been required to participate in training on the new middleware platform and had been provided with the new middleware platform's installation document detailing the scripts to be executed as part of the Migration Exercise.

22 These do not constitute reasonable security arrangements, as expertise *per se* does not render an employee infallible. The Organisation should not have placed all responsibility on the Employee to carry out the API Replication properly, without any accompanying measures to address the risk of human errors, such as independent verification checks[6] or automation of the API Replication process.

23 In connection with the foregoing, the Organisation admitted that, by failing to put in place measures to prevent the Misconfiguration Error from arising, it had contravened the Protection Obligation.

24 Accordingly, the Commission finds that the Organisation negligently breached the Protection Obligation by failing to put in place reasonable security arrangements to mitigate the risk of human error when carrying out the API Replication.

Observations on access control measures

25 Given that the threat actor's initial point of entry into the Organisation's system was through the Compromised Accounts, the Commission would make the following observations about the Organisation's access control measures. For the avoidance of

[6] See *Re E-Commerce Enablers Pte. Ltd* [2023] SGPDPC 6 at [16-18].

doubt, these observations are made solely to provide guidance, and (1) do not constitute additional findings of breaches of the Protection Obligation by the Organisation in this case; or (2) factor in any way in the Commission's final decision in this case.

26 When developing access control measures to safeguard personal data, Organisations are required to implement basic password requirements such as a minimum password length and complexity[7]. The Organisation's Password Policy mandated that default SRL account passwords comprised of 4 digits based on the member's birthdate with no requirement for change on first use, which was a weak password policy that made it relatively easy for threat actors to decipher and left the SRL accounts vulnerable to password spray attacks. At the same time, the Commission acknowledges that by using segregated and differentiated access controls for different types of data, the Organisation imposed stronger guardrails on more sensitive data, thus limiting the impact of a breach of the SRL accounts to six accounts. But for the Misconfiguration Error, the threat actor would not have been able to access the bulk of the Affected Data even after accessing the Compromised Accounts.

[7] See ICT Guide.

27 That said, it was not necessary for the Commission to make any breach findings in relation to the access control measures employed by the Organisation.

The Commissioner's Preliminary Decision

28 In determining whether the Organisation should be required to pay a financial penalty under section 48J of the PDPA, and the amount of financial penalty imposed (if any), the factors listed at section 48J(6) of the PDPA were considered.

Factors considered by the Commission

29 In terms of the nature, gravity and duration of the non-compliance by the Organisation, the Organisation's breach of the Protection Obligation led to the unauthorised access and disclosure of personal data relating to 665,495 individuals, which was voluminous. The Commission further notes that the vulnerability occasioned by the Misconfiguration Error was present for at least 6 months (from March to October 2023), and that the Affected Data was exfiltrated and put up for sale on the dark web.

30 The Commission recognises that:

(a) The Organisation had otherwise implemented adequate and appropriate security arrangements to protect the personal data in its possession and/or under its control;

(b) The Organisation took prompt actions after being alerted about the Incident to mitigate the effects of the Incident and to prevent a recurrence;

(c) Investigations were handled under the Expedited Decision Procedure, under which the Organisation admitted to the facts set out in this decision and to its contravention of the Protection Obligation; and

(d) The Organisation was cooperative with the Commission's investigations.

The Organisation's Turnover

31 In assessing what amount of financial penalty would be proportionate and effective to deter non-compliance with the PDPA, the Commission also took into account the Organisation's annual turnover in Singapore, based on the Organisation's audited accounts.

32 Effective 1 October 2022, the maximum financial penalty imposable for contraventions of any provision in Parts 3 to 6A of the PDPA (the **"Data Protection Obligations**") by organisations whose annual turnover in Singapore exceeds $10 million, has been raised from $1 million to 10% of an organisation's annual turnover in Singapore[8].

33 This increase in the maximum imposable financial penalty evinces Parliament's intent to sharpen the Commission's teeth in order to signal the importance of data protection in the burgeoning digital economy. As explained by then-Minister for Communications and Information at the Second Reading of the Personal Data Protection (Amendment) Bill:

> "**The objective here is to ensure that we achieve the requisite deterrent effect on organisations…** The proposed maximum financial penalty is comparable with other domestic legislation such as the Telecommunications Act and Competition Act and **signals that data protection is of that level of importance in the digital economy.**"
>
> (emphasis added)

[8] See section 48J(3)(a) of the PDPA read with regulation 10A(1) of the Personal Data Protection (Enforcement) Regulations 2021.

34 Given the considerable size of the Organisation's annual turnover in Singapore, the Commission considers that a proportionately higher financial penalty is necessary to serve as an effective deterrent to both the Organisation, and other organisations with turnovers of similar size.

35 This is consistent with the Commission's approach in recent decisions following the raising of the maximum amount of financial penalty[9], and was recently articulated in *Re Keppel Telecommunications & Transportation Ltd* [2024] SGPDPC 3 ("***KTT***") at [40]:

> "In quantifying the financial penalty to be imposed in any given case, the Commission **aims to strike a careful balance between an amount that is (i) proportionate to the circumstances and effect of the organisation's non-compliance with the PDPA but (ii) that remains effective as a deterrent when considering the means of the organisation.** In the present case, upon a consideration of all the factors listed under section 48J(6) of the PDPA, the Commission is of the view that a higher financial penalty is warranted to ensure that the financial penalty meted is proportionate in light of the Organisation's long period of non-compliance with the Protection Obligation (including during

[9] See *Re Fullerton Healthcare Group Pte Limited and Agape CP Holdings Pte Ltd* [2023] SGPDPC 5 at [39], *Re Autobahn Rent A Car Pte Ltd* [2023] SGPDPCS 4 at [11], *Re Century Evergreen Private Limited* [2023] SGPDPCS 5 at [11].

the Migration exercise in May 2020 and again during the Divestment in July 2022) and the type and nature of the personal data affected. **A higher financial penalty is also warranted to ensure that the financial penalty meted will be effective in ensuring future compliance with the PDPA and to achieve the requisite deterrent effect.**"

(emphasis added)

36 Going forward, errant organisations should expect that the size of their annual turnover will continue to be a factor in the Commission's assessment of the amount of financial penalty to be imposed.

37 Having considered all of the matters set out above, the Commissioner preliminarily determined that the Organisation should pay a financial penalty of $450,000.

38 In view of the remedial actions already been taken by the Organisation, no further directions needed to be issued to the Organisation.

Representations made by the Organisation

39 The Organisation was notified of the preliminary decision by way of the Commission's letter dated 13 September 2024 and was invited to make representations. On 27 September 2024, the Organisation made representations to the Commission ("**Representations**") to clarify certain facts stated in the preliminary decision, some of which the Commission accepts and has amended accordingly in this decision. The Organisation also disputed the Commission's imposition of a financial penalty, and in the alternative, the amount of the financial penalty. The Organisation contended that:

(a) The Commission was not empowered to impose a financial penalty under section 48J(1) of the PDPA, as the Organisation had not breached the Protection Obligation "negligently";

(b) Alternatively, even if the Commission was empowered to impose a financial penalty, the Commission erred in law by taking into consideration the Organisation's annual turnover in Singapore when calculating the amount of the financial penalty. Doing so caused the amount of the financial penalty imposed to be inconsistent with the

financial penalties imposed in previous similar cases, which were not calculated with reference to the relevant organisations' turnover; and

(c) Regardless of whether the Commission was empowered to take into consideration the Organisation's turnover, the amount of the financial penalty imposed should be reduced as the Commission's preliminary decision did not sufficiently account for relevant mitigating factors.

40 The Commission shall address each of these representations in turn.

Representation 1: The Commission erred in determining that the Organisation contravened the Protection Obligation negligently

41 Under section 48J(1)(a) of the PDPA, the Commission may require an organisation to pay a financial penalty if it is satisfied that the organisation intentionally or negligently contravened any of the Data Protection Obligations. The Organisation contends that while it did breach the Protection Obligation, its breach was not "negligent" in the meaning of section 48J(1)(a). The Organisation's position is that:

(a) An organisation only breaches the Protection Obligation negligently if it ought to have known at the relevant time that its conduct would result in

unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data in its possession, or similar risks (the "**Risks**").

(b) The Organisation bases this position on the Competition and Consumer Commission of Singapore's ("**CCCS**") *Guidelines on Directions and Remedies* (effective 1 February 2022) ("**CCCS Guidelines**"), arguing that the same legal standard should be adopted for both the PDPA and the Competition Act 20024. The CCCS Guidelines state CCCS' position that a relevant infringement under the Competition Act 2004 is committed negligently "where an undertaking ought to have known that its agreement or conduct would result in a restriction or distortion of competition" (the "**CCCS Standard**")*;*

(c) While the Organisation admits that the measures it adopted fell short of what was required by the Protection Obligation, it nevertheless acted reasonably and was not negligent in relation to its conduct of the Migration Exercise and API Replication:

i. The Organisation had implemented various security arrangements to ensure that the Affected Data was adequately protected, including testing and vulnerability assessments[10]:

ii. There was no alternative to manually creating the Inventory Listing and carrying out the API Replication. Whilst the Organisation does not dispute that, in general, deployment processes should be automated to minimise human errors, there were technical limitations on the extent to which this could have been done for the Migration Exercise. Other aspects of the deployment were carried out using the Organisation's standard processes, which involved automation, and such processes also had controls in place to minimise vulnerabilities; and

iii. The Organisation had assigned the Employee, the most qualified person with the relevant expertise, to lead the team in the API Replication. In light of the Employee's high level of expertise and consistent good performance, as well as the nature of the Inventory Listing task, the Organisation argued that it could not be said that the Organisation ought to have known at the time that

[10] See [16] above.

there was a need to have separate independent verification of the Employee's work. The Organisation was also reasonable in its belief at the time that it would be unnecessary to have other less qualified personnel carry out checks on the Employee's work throughout the Migration Exercise as a whole.

The Commission's decision on whether the Organisation breached the Protection Obligation negligently

42 As a preliminary point, the Commission's view is that the CCCS Standard suggested by the Organisation would not be appropriate in the context of the Protection Obligation.

43 First, the CCCS Standard relates to infringements under the Competition Act 2004 where undertakings (a) enter into anti-competitive agreements[11], (b) abuse a dominant market position[12], or (c) enter into anti-competitive mergers[13] ("**the Competition Infringements**"). The Competition Infringements all concern specific prohibited conduct relating to definitive competition-related harms (e.g. entering into an anti-competitive merger). These are conceptually distinct from the Risks which are not predicated on the occurrence of specific conduct.

[11] Section 34 of the Competition Act 2004.
[12] Section 47 of the Competition Act 2004.
[13] Section 54 of the Competition Act 2004.

44 Second, the Commission also disagrees with the Organisation's application of the CCCS Standard to suggest that negligence would only be found if an organisation ought to have known that its conduct would result in the Risks (i.e. its conduct would necessarily result in unauthorised access or collection of the Affected Data). This appears to conflate negligence with the more stringent standard of recklessness, which applies when a person fails to address risks that are blatant or obvious[14] and does not apply here.

45 The applicable standard for negligence must be grounded in how the Protection Obligation operates. A non-compliance with the Protection Obligation arises where an organisation fails to implement security arrangements that it reasonably should have, considering the Risks posed to the personal data in its possession or under its control. There are two aspects to this, both evaluated on an objective standard – (a) what are the reasonably foreseeable risks posed to the personal data in the organisation's possession or under its control, and (b) what security arrangements should the organisation have reasonably implemented to protect the personal data in its possession or under its control from the said risks.

[14] *Public Prosecutor v Hue An Li* [2014] 4 SLR 661 at [45] and [49].

46 The nature of the risks posed to personal data in an organisation's possession or under its control can be assessed based on a variety of factors including (a) the volume, type and nature of the personal data, (b) the manner in which the personal data is processed and the degree of risk such processing might entail, (c) the form in which the personal data was collected or stored, and (d) the impact that unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data would have on data subjects[15]. The Commission's ICT Guide provides guidance on the data protection practices which organisations should have regard to when implementing security arrangements to address these risks.

47 An organisation which breaches the Protection Obligation, fails to implement measures that a reasonable organisation in its position would, having regard to the foreseeability of the risk and the adequacy of the safeguards in place. If the risk was reasonably foreseeable and the security arrangements (or lack thereof) to reduce, mitigate or eliminate that risk fell below the standard expected of a reasonable organisation, the breach would necessarily be negligent.

48 With these principles in mind, the Commission now turns to consider whether the Organisation had committed a negligent breach of the Protection Obligation.

[15] Advisory Guidelines on Key Concepts in the PDPA (Revised 1 October 2021) at [17.2].

Was the Organisation negligent in failing to implement reasonable security arrangements to prevent the Misconfiguration Error?

49 The Organisation has explained in its representations that the API Replication could not be automated and had to be done manually, since the old middleware platform could not automate the extraction of the existing API configuration. While the Commission accepts this explanation, the Commission is unable to accept the rest of the Organisation's representations on this issue and maintains its finding that the Organisation negligently breached the Protection Obligation within the meaning of section 48J(1)(a) of the PDPA.

50 First, the manual nature of the Inventory Listing made it more susceptible to risks of human error including inadvertent omissions of APIs or calling app IDs, or inaccuracies in the items recorded. This called for more robust systemic processes to mitigate these risks beyond placing the burden on one employee at one single point of failure. The Protection Obligation requires the instituting of security arrangements, or in other words, a safe system to protect personal data from the carelessness of individual persons.

51 If an API was omitted during the Inventory Listing, the Organisation had no other downstream arrangements whether during the Migration Exercise or six months

after the new middleware platform had gone live, to detect this omission and reinstate any relevant security policies or controls in relation to the omitted API. Once an omitted API is not subject to the Organisation's security policies or controls, it becomes more vulnerable to external cybersecurity threats targeting its personal data assets through this API. It was thus entirely foreseeable that errors or omissions in the Inventory Listing could lead to vulnerabilities that could be exploited by a threat actor to circumvent its cybersecurity defences and gain unauthorised access to the Affected Data. In particular:

(a) The Organisation admits that this was the first ever middleware migration it was performing, and it had "no SOPs per se" for such a process. It called this an "exceptional, large-scale" and "complex exercise" that involved implementing a hybrid cloud and on-premises API management platform with API policies and configuration for the migration of middleware. Given that the API Replication was a new and complex undertaking for the Organisation, and the volume of personal data in the Organisation's possession, the Organisation should reasonably have taken greater care to implement robust security arrangements and secondary checks at each critical stage, especially for manual steps. For example, the Organisation could have carried out a security test after the Migration Exercise was concluded to detect cybersecurity vulnerabilities

that may have arisen due to human error, instead of waiting for routine security testing to take place months after deployment.

(b) The APIs are part of the Organisation's network architecture which, if left unprotected, would be targeted by threat actors. It was foreseeable that an omission during the creation of the Inventory List and subsequent API Replication would mean that the Organisation's security arrangements would not have applied to the orphaned API, exposing the Organisation's personal data to the Risks. This omission can be seen as analogous to an organisation's failure to accurately maintain a personal data asset inventory to ensure that the said assets are covered by the organisation's security policies: see *Eatigo International Pte. Ltd. [*2022] SGPDPC 9 at [15] to [16]. Similarly, one key reason for carrying out the API Replication was to ensure that the Organisation had full visibility of all the APIs in its middleware platform after the Migration Exercise was complete, so that it could implement its extant security arrangements (including the Token Verification Policy) on all APIs post-migration to protect the APIs from cybersecurity risks.

(c) In fact, the Organisation had undertaken a threat risk assessment in January 2022 i.e. before embarking on the Migration Exercise (as recorded in its Threat Risk Assessment Report). The Organisation had

flagged misconfiguration of API settings as a risk as "**misconfigured API settings can not only expose sensitive user data**, but also system details that may lead to full server compromise". The risk of an API misconfiguration leading to the compromise of personal data in the Organisation's possession was therefore entirely foreseeable by the Organisation, including more broadly, omissions during coding.

52 On balance, a reasonable organisation ought to have foreseen that an omission in assembling the Inventory List manually, especially in a new and complex middleware migration, might create a cybersecurity vulnerability with foreseeable ramifications for personal data security. This is not a risk that is only discernible upon a retrospective assessment, as evidenced by the Organisation's own Threat Risk Assessment Report. While the Commission accepts the Organisation's representation that the API Replication could not have been automated, given the foreseeable risk of human error inherent in the manual process and the risks posed to the Affected Data in turn, it was unreasonable for the Organisation to rely solely on the Employee to carry out the API Replication, without any meaningful layer of checks on the correctness of the Inventory List, APIs and calling app IDs in the new middleware platform, before it went live.

53 Second, the Employee's expertise and experience *per se* were an insufficient basis for the Organisation to rely solely on the Employee to conduct the Inventory Listing and API Replication without instituting any meaningful secondary checks. As stated at [18] to [22] above, it was not reasonable for the Organisation to make the Employee responsible for the API Replication without further checks.

54 Third, while the Organisation claims it conducted extensive pre-deployment checks and post-deployment penetration testing on the new middleware platform, there is no indication that any of these tests could have detected an omission in the Inventory List and the Misconfiguration Error.

55 The Organisation's approach meant that the Misconfiguration Error would not have been detected *unless*, as it happened, it was exploited by a threat actor in a data breach, or full penetration testing was conducted. The Organisation explained that it did not perform the latter because, among other things, it did not consider that there to have been any change in the security parameters in the new middleware platform. This assumption rested on the false premise that the Employee's Inventory List was accurate and complete. The Commission does not accept that the Organisation could not take reasonable steps to prevent the unauthorised access to the Affected Data. Had the Organisation taken steps to minimise the risks of human error during the API Replication by way of additional checks, it would likely have detected the

Misconfiguration Error. The Commission maintains its finding that the Organisation contravened the Protection Obligation negligently. Accordingly, the Commission is empowered to require the Organisation to pay a financial penalty pursuant to section 48J(1) of the PDPA.

Representation 2: The Commission erred in law by taking into consideration the Organisation's turnover in Singapore when determining the amount of financial penalty to be imposed

56 The Organisation separately contends that the Commission erred in law by taking the size of the Organisation's turnover into account when calculating the financial penalty to be imposed. While the Organisation makes several arguments in this regard, its contentions broadly fall into 2 categories:

(a) ***Ultra vires*:** The Organisation says that section 48J of the PDPA does not empower the Commission to take into consideration the Organisation's annual turnover when determining the amount of the financial penalty to be imposed. It contends that:

i. First, nothing in sections 48J(3) or 48J(6) of the PDPA states that the Commission should take into account an organisation's turnover.

ii. Second, referring to statements made by the then-Minister for Communications and Information and other members of Parliament at the 2nd reading of the Personal Data Protection (Amendment) Bill on 2 November 2020 (the "**PDP (Amendment) Bill 2nd Reading**"), the Organisation suggests that Parliament was "categorical" in explaining that the increased financial penalty cap was intended to ensure that the financial penalties imposed by the Commission were "proportionate to the severity of the data breach". In the Organisation's view, Parliament "did not intend to import a new approach of taking turnover into account as a factor to enhance the quantum of the financial penalty".

iii. Third, taking into account the Organisation's turnover would be contrary to section 48J(6)(h) of the PDPA, under which the Commission must have regard to whether a financial penalty imposed is "proportionate" and "effective" in ensuring compliance and deterring non-compliance with the PDPA. Citing jurisprudence from criminal law, the Organisation contends that proportionality has nothing to do with the means of the infringer, but is solely about whether the severity of the penalty is commensurate with severity of the infringement. Similarly, the

Organisation contends that there is "no principle under Singapore law" that requires the calibration of a penalty based on the means of an organisation to ensure effective deterrence.

iv. Fourth, based on the above, turnover is an "irrelevant" consideration which the Commission does not have the discretion to take into account as a matter of law. The Organisation highlights the CCCS' approach to quantifying financial penalties under the Competition Act 2004 to suggest that the reasons justifying a turnover-based approach in the competition context (to reflect the economic significance of the infringement), do not apply to the PDPA. The Organisation also observes that there are no published decisions arising from other statutory regimes with financial penalty caps based on 10% of an entity's annual turnover in Singapore[16], which lend support to the Commission's approach of scaling financial penalties based on turnover.

(b) **Unequal treatment:** The Organisation also contends that the Commission's decision on the preliminary financial penalty infringed Article 12(1) of the Constitution of the Republic of Singapore ("**Article**

[16] Specifically, section 10(1) of the Telecommunications Act 1999, section 19(c) of the Gas Act 2001 and section 14(c) of the Electricity Act 2001.

12(1)") as it subjected the Organisation to arbitrary discrimination on the basis of its turnover.

i. The proposed financial penalty would result in the Organisation being treated differently from other organisations which were "equivalent or similar save for having a lower turnover". The Organisation refers to the financial penalties previously imposed by the Commission in *SingHealth*[17], *PPLingo*[18], *Eatigo*, and *Carousell*[19] (the **"Precedent Cases**") as evidence of differential and disproportionate treatment.

ii. The differential treatment of the Organisation was not based on legitimate reasons which bore a sufficient rational relation to the objective of section 48J of the PDPA, which in the Organisation's view is to "impose proportionately higher financial penalties for more severe contraventions of the PDPA".

57 The Commission considers each category of the Organisation's representations in turn.

[17] *Singapore Health Services Pte. Ltd. & Ors [2019] SGPDPC 3.*
[18] *PPLingo Pte Ltd* [2023] SGPDPC 12.
[19] *Carousell Pte Ltd* [2023] SGPDPC 13.

The Commission's decision on Organisation's representations regarding ultra vires

58 While the Organisation's representations in this regard attempt to construe the proper scope of the Commission's powers under section 48J of the PDPA, they do not accord primacy to the text of the relevant provisions in the PDPA and their statutory context, over any extraneous material[20].

59 In the Commission's view, the plain language and structure of section 48J of the PDPA clearly demonstrate that the size of an organisation's annual turnover is a relevant factor to be taken into consideration by the Commission when quantifying financial penalties.

60 First, section 48J(3) (read with section 48J(1)(a)) of the PDPA expressly refers to the organisation's annual turnover in Singapore when defining the maximum financial penalty that can be imposed on organisations for breaches of the Data Protection Obligations:

> "**48J. Financial penalties**
>
> (1) Subject to subsection (2), the Commission may, if it is satisfied that —

[20] *Tan Cheng Bock v Attorney General* [2017] 2 SLR 850 ("***Tan Cheng Bock***") at [43].

(a) an organisation has intentionally or negligently contravened any provision of Part 3, 4, 5, 6, 6A or 6B; or

(b) a person has intentionally or negligently contravened —

(i) any provision of Part 9; or

(ii) section 48B(1),

require, by written notice, the organisation or person (as the case may be) to pay a financial penalty.

(…)

(3) A financial penalty imposed on an organisation under subsection (1)(a) must not exceed the maximum amount to be prescribed, which in no case may be more than the following:

(a) in the case of a contravention on or after the date of commencement of section 24 of the Personal Data Protection (Amendment) Act 2020 by **an organisation whose annual turnover in Singapore exceeds $10 million** — **10% of the annual turnover in Singapore of the organisation**;

(b) in any other case — $1 million."

(emphasis added)

61 Under regulation 10A of the Personal Data Protection (Enforcement) Regulations 2021 ("**Enforcement Regulations**"), the maximum amount prescribed for

the purposes of section 48J(3) mirrors the statutory limit set by section 48J(3) of the PDPA:

> "10A. Maximum amount of financial penalties
>
> (1) The maximum amount prescribed for the purposes of section 48J(3) of the Act is —
>
> (a) in the case of a contravention on or after 1 October 2022 by an organisation whose annual turnover in Singapore exceeds $10 million — 10% of the annual turnover in Singapore of the organisation; and
>
> (b) in any other case — $1 million."
>
> (emphasis added)

62 Effectively, section 48J(3) of the PDPA bifurcates organisations that fail to comply with the Data Protection Obligations into two classes – organisations with annual turnover of $10 million and below ("**Low Turnover Class**"), and organisations with annual turnover more than $10 million ("**High Turnover Class**").

(a) Organisations within the Low Turnover Class are subject to a maximum financial penalty of $1 million.

(b) By comparison, regardless of the nature of their non-compliance[21], organisations within the High Turnover Class are subject to higher or lower maximum financial penalties depending solely on the size of their annual turnover. For the High Turnover Class, turnover is obviously one of the relevant considerations for financial penalty quantification, as the larger the turnover, the higher the maximum penalty that can legally be imposed. Whilst this determines the maximum financial penalty that can be imposed, the determination of the actual financial penalty in a given case is a case-specific and multi-factorial exercise that the Commission will elaborate on below.

(c) If Parliament did not intend for turnover to be a relevant consideration in quantifying financial penalties for the High Turnover Class, there would have been no need for section 48J(3) of the PDPA to refer to turnover at all. A higher penalty dollar amount could have been stipulated instead.

(d) This is what was done for financial penalties imposable for contraventions of the obligations under Part 9 of the PDPA ("**the Do Not Call Obligations**"). Under section 48J(4) of the PDPA, the maximum financial penalties imposable on any persons (regardless of turnover) for

[21] For completeness, section 48J(5) of the PDPA does contemplate that different maximum amounts may be prescribed in respect of contraventions of different provisions of the PDPA. However, no such differentiated maximum amounts have been prescribed.

contraventions of the Do Not Call Obligations are expressed as a fixed dollar amount:

> "(4) A financial penalty imposed on a person under subsection (1)(b)(i) must not exceed the maximum amount to be prescribed, which in no case may be more than the following:
>
> (a) in the case of an individual — $200,000;
>
> (b) in any other case — $1 million."

63 Second, contrary to the Organisation's suggestion, the fact that turnover is not specifically identified in section 48J(6) of the PDPA does not mean that it is irrelevant for the exercise of the Commission's discretion when determining the amount of financial penalty to be imposed. Section 48J(6)(j) of the PDPA also requires the Commission to consider any other matter that may be relevant when determining the amount of financial penalty imposed, which clearly signals that the factors set out in sections 48J(6)(a) to (i) of the PDPA are not intended to be the only factors that the Commission may consider. Such a narrow reading of the provision would render section 48J(6)(j) of the PDPA otiose.

64 The Commission must have regard to all of the matters listed in section 48J(6) of the PDPA when quantifying financial penalties for contraventions of both the Data Protection Obligations and the Do Not Call Obligations. In this context, it is understandable why the list of matters at section 48J(6) of the PDPA does not make explicit reference to turnover, if Parliamentary intent was that turnover be less relevant of a factor for breaches of the Do Not Call Obligations.

65 Third, section 48J(6)(h) of the PDPA obliges the Commission to consider whether the amount of the financial penalty to be imposed will be effective in deterring non-compliance with the PDPA. This limb reflects the over-arching purpose of deterring non-compliance with the PDPA amongst all organisations generally. Unlike the other sub-provisions of section 48J(6) of the PDPA, which refer to "the organisation" (i.e. the organisation that has contravened the PDPA), section 48J(6)(h) of the PDPA describes "deterring non-compliance with this Act" generally, and without reference to the specific organisation that is subject to the financial penalty.

66 In this context, the Commission agrees with the Organisation that "deter" in the meaning of section 48J(6)(h) of the PDPA refers to both specific deterrence (i.e. deterring the organisation's own ongoing or future non-compliance with the PDPA), and general deterrence (i.e. deterring other organisations from non-compliance with the PDPA). The Commission addresses both facets below.

Specific deterrence

(a) The Organisation represents that the need for specific deterrence only arises if there is a risk of an organisation re-infringing, and the size of an organisation's turnover has no bearing on this. The Organisation further suggests that the Commission already has powers to address an organisation's risk of re-infringement by issuing directions under section 48I of the PDPA.

(b) This broad characterisation does not obviate the need to consider an organisation's annual turnover, and misses what specific deterrence is about in the context of section 48J(6)(h) of the PDPA. Once the Commission is satisfied that the organisation's contravention of the Data Protection Obligation(s) was intentional or negligent pursuant to section 48J(1)(a) of the PDPA, it exercises its discretion to determine whether to impose a financial penalty on the organisation. Once it decides to do so, the Commission would then have regard to the factors listed in section 48J(6) of the PDPA in "determining the amount of a financial penalty imposed under [section 48J(1)]". Specific deterrence is taken into consideration when quantifying the <u>amount</u> of the financial penalty to be imposed. In the context of section 48J(6)(h) of the PDPA, this is an issue

of weight, and not relevance (i.e. whether a financial penalty should be imposed at all).

(c) The Commission accepts that there are factors which would go towards lowering the weight to be placed on specific deterrence in a given case. These include where (i) an organisation voluntarily admits to, and accepts responsibility for its non-compliance with the PDPA, and/or (ii) voluntarily implements remedial measures to correct its non-compliances with the PDPA without the need for the Commission to issue directions to this effect under section 48I of the PDPA. The Commission has already taken these factors into account to reduce the financial penalty imposed on the Organisation in this case.

General deterrence

(d) For the financial penalty to serve as an effective general deterrent, it must signal to organisations of similar size and circumstances that contraventions of the PDPA will attract financial penalties of a level that would dissuade such organisations from non-compliance. For organisations in the High Turnover Class particularly, low financial penalties that do not consider the sizes of their annual turnover may not sufficiently dissuade them from non-compliance if the financial penalty can be factored as a cost of business. The Commission elaborates on

this below in the context of considering relevant extraneous materials that confirm this position.

67 Fourth, section 48J(6)(i) of the PDPA obliges the Commission to consider the likely impact of the imposition of the financial penalty on an organisation, including the ability of the organisation to continue its usual activities. The financial penalty meted out should avoid imposing a crushing burden or cause undue financial hardship to the organisation. To assess how the imposition of a financial penalty may affect an organisation's ability to continue operating its business, the Commission must necessarily consider the organisation's financial means, including the size of its turnover. If the Commission assesses that imposition of a financial penalty may lead to financial distress and closure of the organisation's business, the Commission may reduce the financial penalty quantum to avoid imposing a crushing burden on the organisation. If turnover and the financial means of organisations are not relevant to determining the amount of financial penalties, the Commission would not be able to give effect to section 48J(6)(i) of the PDPA.

68 Fifth, section 48J(5A) of the PDPA provides that for the purposes of determining the maximum financial penalty imposable on organisations in the High Turnover Class,

an organisation's annual turnover is to be ascertained from its most recent audited accounts at the time the financial penalty is imposed[22].

69 The fact that the relevant turnover to be considered is the turnover at the time of imposition of the financial penalty (and not, for example, the organisation's turnover at the time its contraventions were committed), supports that the financial penalty is about deterring ongoing or future contraventions, and not about approximating economic harms that result from such contraventions. Where an organisation gains a financial benefit or avoids a financial loss as a result of its non-compliance, this is taken into account as a separate factor under section 48J(6)(c) of the PDPA.

70 Sixth, there is nothing in the language or structure of section 48J of the PDPA that supports the Organisation's suggested interpretation that turnover is only a relevant consideration in the context of "severe breaches". In the Commission's view, this is too narrow a reading of section 48J of the PDPA based on its unambiguous plain language. The primary source of information as to the legislative intent should be the text of the provision itself, and extraneous material should not be used to call the ordinary meaning of a statutory provision into question[23].

---

[22] See section 48J(5A) of the PDPA: "For the purposes of subsections (3)(a) and (4A)(b), the annual turnover in Singapore of an organisation or a person (as the case may be) is the amount ascertained from the most recent audited accounts of the organisation or person available at the time the financial penalty is imposed on that organisation or person."
[23] *Tan Cheng Bock* at [45] to [48].

71 In any event, the relevant extraneous material either confirms that turnover is a relevant factor in determining financial penalties to be imposed under section 48J of the PDPA, or does not support the view proposed by the Organisation (i.e. that Parliament's intent in amending section 48J of the PDPA was only for the Commission to impose proportionately higher financial penalties for more severe breaches).

Ministerial statements at PDP (Amendment Bill) 2nd Reading

72 Contrary to the Organisation's representations, the statements made by the then-Minister at the PDP (Amendment) Bill 2nd Reading confirm that the objective behind increasing the financial penalty cap when the PDPA was amended in 2021 was to enhance the effectiveness of the Commission's enforcement overall and not to limit higher financial penalties only to "severe" cases:

(a) In introducing the category of amendments including what is now section 48J, the then-Minister framed the over-arching purpose of these amendments as being to enhance the effectiveness of the Commission's enforcement. At the end of his opening speech, the then-Minister emphasised that the amendments to the PDPA were about creating greater organisational accountability for personal data, so as to enhance Singapore's status as a global hub for data flows and digital transactions.

This point was once again emphasised in the then-Minister's closing speech, where he explicitly framed the increase as being about creating market incentives to motivate organisations to adopt better data protection standards in general, and not just about taking stronger enforcement action in "severe" cases:

> "Sir, I will elaborate on the amendments which aim to: first, strengthen consumer trust through organisational accountability; **second, ensure effective enforcement**; third, enhance consumer autonomy; and fourth, support data use for innovation.
>
> (…)
>
> Sir, let me now move to the second cluster of amendments, which seeks to **enhance the flexibility and effectiveness of the PDPC's enforcement**."
>
> (…)

> "Sir, in summary, the proposed amendments to the PDPA will strengthen consumer trust with greater accountability for the protection of personal data; it will give greater certainty for organisations to use data for legitimate business purposes with the requisite safeguards; and it will ultimately enhance

Singapore's status as an important node in the global network of data flows and digital transactions. Sir, I beg to move."

(…)

"To support that and to ensure organisations take their obligations to protect data seriously, we are introducing both incentives and penalties – carrots and sticks, if you will. The PDPC will issue new advisory guidelines with examples and illustrations, so that organisations have ample notice of the expected standard of conduct.

(emphasis added)

(b) When later presenting the specific amendments that introduced section 48J, the then-Minister did record that the Commission would ensure that financial penalties would be proportionate to the severity of data breaches. However, this was in the specific context of pre-empting concerns heard during public consultations about the increase in the financial penalty cap, and not for the purposes of framing the purpose or object of the amendments as a whole. Contrary to the Organisation's suggestion, the Commission is unable to read into this statement any suggestion that higher financial penalties (calculated with reference to an organisation's turnover) would only be imposed in "severe" cases:

"Clause 24 increases the maximum financial penalty for breaches of Parts III to VI, and the new Parts VIA and VIB, to 10% of an organisation's annual turnover in Singapore or $1 million, whichever is higher. This penalty framework is similar to that in other domestic regulation and legislation, including the Competition Act and the Telecommunications Act.

During public consultations, concerns were raised about the higher financial penalties. I would like to assure Members, as well as the broader community, that the PDPC will ensure that financial penalties imposed are proportionate to the severity of the data breach. The Bill also provides for Ministerial discretion to review the effective date for these penalties to commence and we intend for the revised financial penalty cap to take effect no earlier than one year after the Act comes into force.

…

As data breaches cannot always be prevented, the PDPC's enforcement framework reinforces the importance of dealing expeditiously with data breaches to reduce harm, through measures like breach reporting and statutory undertakings.

Last year, PDPC investigated 185 cases, issued 58 decisions and ordered 39 organisations to pay a total of $1.7 million in financial penalties and that includes the highest financial penalty sums the PDPC imposed in 2019, which were $750,000 and $250,000 on IHiS and SingHealth respectively.

The Bill enhances PDPC's investigation powers and raises the financial penalty cap, to improve the effectiveness of PDPC's enforcement.

We are also creating market incentives, which can motivate organisations to practise high standards of data protection."

(emphasis added)

(c) Member of Parliament Mr Desmond Choo had earlier asked the then-Minister whether the increased financial penalty cap would put Singapore at a comparative economic disadvantage to other Asian jurisdictions which subjected organisations to lower maximum financial penalties, and asked the then-Minister to reconsider re-aligning the

maximum financial penalty to be in line with other Asian jurisdictions[24]. In responding to Mr Desmond Choo's question in his closing speech, that the then-Minister spoke about the "reasonableness" of the increased financial penalty cap, and reiterated that the objective was to achieve the requisite deterrent effect on organisations. This suggests that the "requisite" or appropriate deterrent effect could only be achieved by way of a maximum financial penalty expressed as a percentage of an organisation's annual turnover (introduced in the new section 48J of the PDPA), and not a fixed amount as was the case with the examples of Malaysia, Hong Kong and Philippines raised by Mr Desmond Choo:

> "There are some concerns about the reasonableness of the increased financial penalty cap. Mr Desmond Choo proposed aligning the financial penalty cap with other Asian jurisdictions.

[24] "My third point of clarification relates to the increased financial penalties under the amendments. The maximum financial penalty that can be meted out is a fine amounting to 10% of the defaulting organisation's annual turnover in Singapore. For comparison, the contravention of Personal Data Laws in Hong Kong attracts a maximum financial penalty of HKD$1 million; in Malaysia it is RM$300,000 and in the Philippines, it is PHP$5 million.

The worry, which has been similarly reflected during the public consultation, is that the maximum fine that can be imposed might be too large compared to worldwide standards, especially in Asia. Could this disadvantage Singapore as an offshore destination, where MNCs might choose other Asian countries over ours to set up operations? While the penalty imposed on a contravening organisation will vary naturally according to the facts, this might artificially create the impression that the financial penalties under Singapore's data privacy regime are much harsher compared to those of its neighbours. In light of this, can the Ministry reconsider the maximum financial penalty that it is imposing on defaulting organisations to better align with the standards in neighbouring Asian jurisdictions or competing economies?"

> The objective here is to ensure that we achieve the requisite deterrent effect on organisations. And that is why the financial penalties have been calibrated in the way that I have described. The proposed maximum financial penalty is comparable with other domestic legislation such as the Telecommunications Act and Competition Act and signals that data protection is of that level of importance in the digital economy."
>
> (emphasis added)

(d) In referring to the equivalent financial penalty caps under the Telecommunications Act 1999 and Competition Act 2004, the then-Minister was not suggesting that the same policy considerations underpinned their respective financial penalty regimes. The then-Minister was simply referring to these regimes as domestic examples of financial penalty caps based on turnover, which supported the "reasonableness" of the proposed financial penalty cap under the PDPA.

(e) In all, the Commission is unable to glean from the Parliamentary excerpts cited by the Organisation any support for its proposed reading of Parliamentary intent.

Closing Note to Public Consultation on Draft Personal Data Protection (Amendment) Bill

73 Second, contrary to the Organisation's representations, the statements made by the then-Ministry of Communications and Information ("**MCI**") and the Commission in their closing note to the public consultation on the proposed amendments to the PDPA issued on 5 October 2020 ("**Closing Note**")[25] do not convey any intent for consideration of an organisation's turnover to be limited to only "severe" cases. The Commission stated that in a given case, the appropriate financial penalty would be determined based on a variety of relevant factors including the facts of the individual case, the seriousness of the breach and its impact, the level of the organisation's culpability, the need for deterrence, and the overall proportionality of the amount. This is consistent with the existing structure of section 48J of the PDPA outlined above, and does not amount to any representation on the Commission's part that an organisation's turnover would play a limited or specific role in the exercise of the Commission's discretion when quantifying financial penalties.

[25] https://pdpc.gov.sg/guidelines-and-consultation/2020/05/public-consultation-on-personal-data-protection-(amendment)-bill

(a) The relevant section of the Closing Note which pertained to feedback received on the increased financial penalty cap is reproduced below in full:

> **"Increased Financial Penalty Cap**
>
> 6. MCI/PDPC proposed to increase the maximum financial penalty for data breaches under the PDPA to (i) up to 10% of an organisation's annual turnover; or (ii) S$1 million, whichever is higher. The higher cap is intended to serve as a stronger deterrent and enable PDPC to take effective enforcement action based on the circumstances and seriousness of a breach, in order to uphold organisational accountability for personal data.
>
> 7. Approximately a third of all the respondents were concerned with the increase in the financial penalty cap, with some citing the economic downturn arising from COVID-19. Some respondents also requested for a sunrise period before the increased financial penalty cap takes effect. There were also several respondents who requested that MCI/PDPC make clear in the draft PDP (Amendment) Bill that the financial penalty cap refers to 10% of

an organisation's annual turnover **in Singapore**; or S$1 million, whichever is higher.

8. MCI/PDPC notes organisations' feedback and will take into account the prevailing economic situation in refining the financial penalty framework. Regardless of the higher cap, in determining the appropriate financial penalty quantum, PDPC will continue to be circumspect and guided by the facts of the individual case, as well as relevant factors including the seriousness of the breach and its impact, level of culpability, the need for deterrence, and the overall proportionality of the amount.

9. In determining the financial penalty quantum, PDPC currently considers factors such as whether the organisation took any action to mitigate the effects of the data breach and the type and nature of the personal data affected. Some of these factors are listed in the Guide on Active Enforcement. To provide clarity and regulatory certainty, MCI/PDPC intends to set out in the PDPA a non-exhaustive list of factors that PDPC would consider and give weight to as appropriate when determining the quantum of financial penalty to impose.

10. MCI/PDPC also intends to amend the draft PDP (Amendment) Bill to expressly state that the maximum financial penalty for the DP Provisions is (i) up to 10% of an organisation's annual turnover in **Singapore**; or (ii) S$1 million, whichever is higher. MCI/PDPC intends to have tiered financial penalty caps for breaches of the DNC provisions, aligned with the egregiousness of the breach."

(emphasis added)

(b) Nothing in the above supports the Organisation's suggestion that consideration of turnover was only intended to be limited to "severe" cases.

(c) While the Organisation claims that the Closing Note "specifically emphasises that the appropriate financial penalty quantum (would be) tied to the egregiousness of the breach", the Commission notes that the statement cited by the Organisation at paragraph 10 of the Closing Note was made in respect of the Do Not Call Obligations, which are not subject to a turnover-based financial penalty cap. In any event, the Commission sees no inconsistency with the egregiousness of an

organisation's breach being one determining factor in the amount of any financial penalty imposed.

Decision of the CCCS in quantifying financial penalty under the Competition Act 2004

74 Third, the Organisation argued that CCCS' rationale for calculating financial penalties based on an undertaking's turnover does not apply to the PDPA context. In the Organisation's view, unlike the PDPA, the size of the undertaking is directly relevant to the economic harm caused to the relevant market by the Competition Infringements and therefore "directly correlate to the severity of the infringement itself". The Organisation referred the Commission to the CCCS' decision in *Collusive Tendering (Bid-Rigging) for Termite Treatment/Control Services by Certain Pest Control Operators in Singapore CCS 600/008/06* (9 January 2008) (**"Pest Control Operators"**) to illustrate the abovesaid point.

75 While the Commission agrees that the Competition Infringements address conceptually different harms from the Data Protection Obligations, a closer examination of CCCS' decision in Pest Control Operators reveals that CCCS also compared the proposed financial penalty against the size of the undertaking's turnover

in order to ensure that the financial penalty was effective as a deterrent given the relative size and financial position of the undertaking.

> "379. Another factor is whether the financial penalty calculated after adjustment for the duration of infringement represents a relatively low proportion of an undertaking's total turnover, for example, where that undertaking has significant operations in other markets. In such a case, the Commission may consider it necessary to increase the undertaking's penalty at this stage to arrive at a sum that represents, for that undertaking, a significant amount that will act as a sufficient deterrent, having regard to the seriousness of the infringement(s) and the undertaking's total turnover. These points are considered in the detailed assessment in relation to each Party.
>
> …
>
> 382. As for the size of the undertakings in question, the Commission considers that this would have been taken into consideration when applying a percentage rate to each undertaking's relevant turnover as a starting point. The Commission recognises that some Parties are larger than others and where a Party's relevant turnover constitutes a relatively small percentage of its total turnover, the Commission may consider adjustments to ensure that the financial penalties will represent a significant sum and act as an adequate deterrent for

such a Party, having regard to the seriousness of the infringement(s) and the total turnover. As such, the Commission considers that no downward adjustment for smaller Parties would be appropriate at this stage.

383. The Commission notes that the financial position of the Parties is a relevant consideration in determining whether the penalty imposed will be sufficiently deterrent, not only in relation to the Party in question but also in relation to like-minded undertakings which may consider engaging in anti-competitive activities.

…

438. … The Commission is mindful that the financial penalty to be imposed should commensurate with the size and financial position of the undertaking. In this instance, the Commission is of the view that the figure reached after adjustment for duration is not a significant sum in relation to [the undertaking] because both the figure and the relevant turnover taken into account for the starting point represent an inadequate proportion of [the undertaking's] total turnover for the year ending 31 December 2006. In accordance with paragraph 379, in order to achieve the objectives described in paragraph 377, the Commission considers that it is necessary to increase the penalty figure

reached after the adjustment to the duration to give a figure that represents a significant sum to Killem."

(emphasis added; internal citations omitted)

Based on the above, CCCS increased the amount of the financial penalty imposed to a larger percentage of the undertaking's turnover, not simply because turnover correlated to the severity of the anti-competitive infringement, but because the penalty needed to represent a "significant sum" to the undertaking. This is consistent with the Commission's view on the relevance of an organisation's turnover when determining the appropriate amount of financial penalty to serve as an effective deterrent.

76 For all of the above reasons, the Organisation's representations on this issue are not accepted. The Commission maintains that it is relevant to consider the Organisation's turnover in determining the amount of financial penalty to be imposed in this case.

Observation – Decision of the European Data Protection Board construing equivalent provisions under EU's General Data Protection Regulation

77 The Commission also observes that the practice of taking an organisation's annual turnover into account for the purpose of ensuring effective deterrence is consistent with the practices of foreign data protection authorities. Article 83 of the

General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), which bears conceptual similarities to section 48J of the PDPA, has been interpreted by the European Data Protection Board ("**EDPB**") to allow reference to an undertaking's turnover when calculating the size of equivalent administrative fines imposed under the GDPR.

(a) Article 83(1) of the GDPR requires that administrative fines imposed in each individual case be effective, proportionate and dissuasive. The EDPB explained in "*Guidelines 04/2022 on the calculation of administrative fines under the GDPR*"[26] ("**EDPR Fine Guidelines**"), that a fine is effective if it re-establishes compliance with the GDPR, punishes unlawful behaviour, or both[27], and described "dissuasiveness" as being about both general deterrence (discouraging others from committing the same infringement in the future) and specific deterrence (discouraging the addressee of the fine from committing the same infringement again)[28]. This mirrors section 48J(6)(h) of the PDPA.

(b) Similar to section 48J(3) of the PDPA, articles 83(4) to 83(6) of the GDPR create a two-class regime for administrative fines. Undertakings with total worldwide annual turnover of EUR 500 million or less are

[26] https://www.edpb.europa.eu/system/files/2023-06/edpb_guidelines_04022_calculationofadministrativefines_en.pdf
[27] EDPB Fine Guidelines, section 7.1, para 135.
[28] EDPB Fine Guidelines, section 7.3, paras 142 – 143.

subject to maximum fine amounts which are fixed (described as "static maximum amounts")[29]. Undertakings with total worldwide annual turnover of more than EUR 500 million are subject to maximum fine amounts expressed as a percentage of the undertaking's total worldwide annual turnover[30] (described as "dynamic maximum amounts").

(c) Similar to section 48J(6) of the PDPA, article 83(2) of the GDPR lists various factors that EU supervisory authorities must give "due regard to" when deciding on the amount of the administrative fine to be imposed, which largely overlaps with section 48J(6) of the PDPA, and does not explicitly state that the size of an undertaking's annual turnover should be considered when determining the administrative fine quantum.

(d) However, in *EDPB Binding Decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR*[31], the EDPB made clear that the size of an undertaking's turnover was not just relevant to determining the maximum fine that could be lawfully imposed under the GDPR, but was also of relevance in the calculation of the fine amount. The undertaking

[29] EUR 10 million for infringements of the provisions listed in Article 83(4), and EUR 20 million for infringements of the provisions listed in Articles 83(5) and 83(6).
[30] 2% for infringements of the provisions listed in Article 83(4), and 4% for infringements of the provisions listed in Articles 83(5) and 83(6).
[31] https://www.edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf

in question, Whatsapp Ireland Limited ("**WhatsApp IE**"), made arguments that were substantively similar to those made by the Organisation in respect of section 48J of the PDPA:

> "407. WhatsApp IE's position is that "[the] sole relevance of turnover for the purpose of Article 83 GDPR is to ensure that any proposed fine - once calculated - does not exceed the maximum fining caps set out in Articles 83(4) to (6) GDPR." Furthermore, WhatsApp IE states that "turnover is not a relevant factor to take into account as part of the Article 83(2) GDPR assessment" because this provision "prescriptively lists the relevant factors that can be taken into account and the legislature chose not to include turnover as a specific factor". WhatsApp IE rejects the notion that "sensitivity to punishment needs to be taken into account and that the fine needs to have a noticeable impact on the profits of an undertaking", as was raised by the (German Supervisory Authority). Moreover, in WhatsApp IE's view "such an interpretation would be contrary to legal certainty as such a precise factor should have been expressly included in Article 83(2) GDPR"."
>
> (emphasis added)

(e) The EDPB rejected Whatsapp IE's arguments and explained the relevance of turnover, as follows:

> "408. "Turnover" is mentioned explicitly in Article 83(4)-(6) GDPR, in connection with the calculation of the maximum fine amount applicable to undertakings with a total annual turnover in the previous financial year that amounts to more than 500 million EUR (the dynamic maximum fine amount). The aim is clear: to ensure an effective, appropriate and dissuasive fine can be applied to deter even to the largest undertakings. The Guidelines on Administrative Fines state that "[i]n order to impose fines that are effective, proportionate and dissuasive, the supervisory authority shall use for the definition of the notion of an undertaking as provided for by the CJEU for the purposes of the application of Article 101 and 102 TFEU". The connection is made between the size of the undertaking, measured in terms of turnover, and the magnitude a fine needs to have in order to be effective, proportionate and dissuasive. In other words, the size of an undertaking - measured in terms of turnover - matters.
>
> 409. Though it is true that neither Article 83(2) GDPR nor Article 83(3) GDPR refer to the notion of turnover, drawing from this an

absolute conclusion that turnover may be considered exclusively to calculate the maximum fine amount is unsustainable in law. Firstly, including a reference to turnover in these provisions is unnecessary, as on the one hand all fines - whether set close to the upper limit or far below it - must be set at a level that is effective, proportionate and dissuasive (cf. Article 83(1) GDPR), and on the other hand the dynamic maximum fine amount sets out the limits within which the (Supervisory Authorities) may exercise their fining power. Secondly, it would be internally contradictory for the GDPR to introduce a dynamic upper limit to fines, while at the same time prohibiting supervisory authorities from assessing whether a fine might need to be increased or decreased in light of the turnover of a company - again - to ensure it is effective, proportionate and dissuasive (cf. Article 83(1) GDPR).

410. The words "due regard shall be given to the following" in Article 83(2) GDPR by themselves do not indicate the list is an exhaustive one. The wording of Article 83(2)(k) GDPR, which allows for any other aggravating or mitigating factor to be taken into account - even though not explicitly described - supports this view.

411. The application of a dynamic maximum fine amount is not a novelty in EU law, as this is a well- established notion in European competition law. While the EDPB concedes there are differences between both systems, the similarities are such that CJEU case law from the field of competition law may serve to clarify a number of questions on the application of the GDPR. In particular, the EDPB notes that taking into consideration turnover - as one relevant element among others - for the calculation of fines is an accepted practice in the field of competition law.

412. In light of all of the above, the EDPB takes the view that the turnover of an undertaking is not exclusively relevant for the determination of the maximum fine amount in accordance with Article 83(4)-(6) GDPR, but it may also be considered for the calculation of the fine itself, where appropriate, to ensure the fine is effective, proportionate and dissuasive in accordance with Article 83(1) GDPR. The EDPB therefore instructs the (Irish Supervisory Authority) to take this into account in the present case in the context of amending its Draft Decision on the basis of this binding decision."

(emphasis added; internal citations omitted)

(f) In the Commission's view, the reasoning above is equally persuasive in respect of section 48J of the PDPA. It would be internally contradictory for section 48J of the PDPA to set a maximum financial penalty expressed as a percentage of the organisation's turnover, while at the same time prohibiting the Commission from considering that turnover to assess the size of the financial penalty.

The Commission's decision on Organisation's representations on unequal treatment

78 The Organisation cites the Court of Appeal's decision in *Syed Suhail bin Syed Zin v Attorney-General* [2021] 1 SLR 809 (CA) ("***Syed Suhail***") as basis for its arguments that it has been unequally treated in the meaning of Article 12(1). In *Syed Suhail*, the Court of Appeal set out a 2-step framework to determine whether decisions taken by an executive body (such as the Commission) infringed Article 12(1):

(a) First, are the persons allegedly discriminated between equally situated, such that any differential treatment calls for justification? This is a factual enquiry. If the persons allegedly discriminated between are not equally situated, there is no contravention of Article 12(1).

(b) Second, if the persons allegedly discriminated between are equally situated, was differential treatment by the executive body reasonable?

79 Simply put, the *Syed Suhail* test requires persons in *like* situations to be treated alike[32]. Applying the test in *Syed Suhail*, the Commission disagrees that the Organisation has been subject to any unlawful discrimination.

80 First, the Organisation has not identified another equally situated organisation which the Commission has treated differently. While the Organisation asserts that its preliminary financial penalty was higher than those imposed in the Precedent Cases (which concerned breaches of a similar or worse severity), those organisations were not equally situated with the Organisation, as they were subject to a different statutory financial penalty regime.

81 Under section 48J(3) of the PDPA read with regulation 10A of the Enforcement Regulations, for organisations in the High Turnover Class, only contraventions

[32] The Court of Appeal elaborated on the analytical approach to the first step of the Syed Suhail test in *Attorney-General v Datchinamurthy a/l Kataiah* [2022] SGCA 46 at [30]:

> "30 (…) (I)n ascertaining whether persons are equally situated, the court is to have regard to the nature of the executive action in question (…) and consider whether, in that context, the persons being compared are so situated that it is reasonable to consider that they should be similarly treated. Put another way, the test is a factual one of whether a prudent person would objectively think the persons concerned are roughly equivalent or similarly situated in all material respects (…). Here, the notion of being equally situated is "an analytical tool used to isolate the purported rationale for differential treatment, so that its legitimacy may then be assessed properly"; the first limb of the test in (Syed Suhail) being intended to identify the "purported criterion for the differential treatment in question" (…). The subsequent question, under the second limb of the test, would then be whether the differential treatment was reasonable."
>
> (emphasis added, internal citations omitted)

occurring on or after 1 October 2022 are subject to the increased maximum financial penalty of 10% of the organisation's annual turnover in Singapore. In all other cases (including contraventions by organisations in the High Turnover Class which occur before 1 October 2022), the maximum financial penalty remains at S$1 million. The contraventions in the Precedent Cases all occurred before 1 October 2022. Accordingly, even though those organisations were in the High Turnover Class, they were not equally situated with the Organisation under the section 48J regime.

82 Second, it suffices to say that organisations with different sizes of turnover – particularly, organisations within the High Turnover Class with different sizes of turnover - are not equally situated. For the reasons stated above, the size of an organisation's turnover is a relevant factor that informs the exercise of the Commission's discretion under section 48J of the PDPA. If the size of an organisation's turnover is a relevant consideration, differentiating between organisations on the basis of this relevant consideration is legitimate and lawful. The analysis ends at the first stage of the *Syed Suhail* test.

83 Third, even if the Organisation is considered to be equally situated to all other organisations in the High Turnover Class (such that the analysis proceeds to the second stage of the *Syed Suhail* test), differentiating financial penalties based on organisations' turnovers bears a rational relation to, and indeed promotes, section

48J's object of ensuring effective deterrence of contraventions of the PDPA. If the financial penalty is too small, large organisations may simply factor the risk of a low penalty as part of the cost of doing business. This would rob the financial penalty of its intended deterrent effect and be inimical to the aim of ensuring that contraventions of the PDPA do not recur.

84 For the above reasons, the Organisation's representations alleging unequal treatment in the quantification of the preliminary financial penalty are not accepted.

The Organisation's other representation on the use of turnover in determining financial penalties

85 For completeness, the Commission addresses the Organisation's contention that quantifying financial penalties based on turnover may incentivise large organisations to structure their data processing in such a way that would result in smaller subsidiaries being legally responsible for the Data Protection Obligations.

86 To the extent that organisations remain responsible for personal data processed on their behalf and for their purposes by a data intermediary[33], the Commission does not consider this to militate against a turnover-based approach to

[33] Section 4(3) of the PDPA.

quantifying financial penalties. Ultimately, the Commission will scrutinise the substance of the arrangements between organisations and their data intermediaries to determine for whose benefit the personal data is being processed, and where (and to what extent) control resides. Should the Commission determine that organisations have deliberately structured their internal data processing to avoid or minimise liability for poor data protection practices, it will not hesitate to take such conduct into account in determining the amount of any financial penalty imposed.

The Commission's Financial Penalty Framework

87 In its representations, the Organisation suggested that the Commission had determined the preliminary financial penalty arbitrarily and without reference to any objective computation framework. This is not the case, and the Commission takes this opportunity to elaborate on key aspects of its analytical framework for determining the amount of financial penalties to be imposed under section 48J of the PDPA (the "**FP Framework**").

Guiding Principles

88 The Commission is guided by principles distilled from sources including: (a) the language and structure of the PDPA, (b) Parliamentary intent as expressed in the Second Reading speeches during the enactment and amendment of the PDPA, (c)

the practices of foreign data protection authorities in administering similar financial penalty regimes, and (iv) jurisprudence from the Singapore courts in the domain of criminal sentencing (with the necessary adjustments for the difference in statutory context).

89 **Deterrence & Proportionality:** First, as expressed in section 48J(h) of the PDPA, the primary competing considerations at the heart of the FP Framework are that financial penalties must be large enough to deter non-compliance effectively, but not too large such that they are not proportionate to the seriousness of the non-compliance. The Commission acknowledged this inherent tension in *KTT* at [40]:

> "In quantifying the financial penalty to be imposed in any given case, the Commission aims to strike a **careful balance** between an amount that is (i) proportionate to the circumstances and effect of the organisation's non-compliance with the PDPA but (ii) that remains effective as a deterrent when considering the means of the organisation."

90 **Balancing interests:** Second, in considering the relative weight to be given to effective deterrence and proportionality, the Commission must be mindful of the overarching balance that the PDPA itself aims to strike between the right of individuals

to protect their personal data and the need of organisations to collect, use or disclose personal data for legitimate purposes[34].

91 As expressed by the then-Minister during the Second Reading of the Personal Data Protection (Amendment) Bill, the ultimate purpose of effective enforcement of the Data Protection Obligations is to strengthen consumer trust with greater organisational accountability for personal data protection, so as to enhance Singapore's standing as a trusted global hub for international data flows and digital transactions[35]. Put differently, financial penalties imposed under the PDPA are not ends in themselves to punish errant organisations. They are a regulatory tool for organisations to take greater accountability for data protection, which in turn gives individuals greater confidence to entrust their personal data to organisations. Ultimately, this promotes a trusted ecosystem of personal data flows between individuals and organisations.

92 **Like and consistent treatment**: Third, the Commission must give effect to the two-tiered financial penalty regime created by section 48J(3) of the PDPA (i.e. differential treatment of the Low Turnover Class and High Turnover Class). The two-tier regime suggests that the size of an organisation's turnover should be accorded

[34] Section 3 of the PDPA.
[35] See [72(a)] above.

more weight for organisations in the High Turnover Class. Other relevant factors must be given similar weight in similar cases.

93 **Specific application**: Fourth, the FP Framework must not be applied mechanistically without sensitivity to the particular facts and circumstances of a given case. The determination of a financial penalty is a multi-faceted, and necessarily fact-specific exercise. All the factors set out in section 48J(6) of the PDPA, including any other relevant factors not specifically listed therein, must be taken into account. While the principles underpinning the FP Framework must be applied consistently, this is not a mathematical exercise and the Commission must have room to make adjustments and give appropriate weight to factors based on their specific relevance to the organisation and contravention in question[36].

94 While the Commission is sharing details of its FP Framework in order to provide guidance, nothing set out below should be construed as creating any expectation that the Commission will or will not take any particular course of action in a future case, as every case requires individual consideration. The FP Framework is a guide and does not limit or restrict the full extent of the Commission's powers under the PDPA,

[36] Drawing from the principles stated by the High Court in *Syed Fathuddin Putra bin Syed a Rahman v Public Prosecutor and another appeal* [2024] 3 SLR 1672.

particularly in administering and enforcing the PDPA. The FP Framework may be updated and supplemented by the Commission as appropriate.

The FP Framework

95 The Commission's FP Framework consists of a preliminary step followed by a five-step methodology to calculate the appropriate financial penalty.

Preliminary Step – Determining the Case Max FP

96 At the outset, the Commission ascertains the statutory maximum financial penalty ("**Statutory Max FP**") from section 48J(3) of the PDPA:

(a) For organisations in the Low Turnover Class, the Statutory Max FP is $1,000,000; and

(b) For organisations in the High Turnover Class, the Statutory Max FP is 10% of the organisation's annual turnover in Singapore.

97 The Commission then applies a percentage rate or quantum cap not exceeding the Statutory Max FP based on the nature of the organisation's contravention of the Data Protection Obligations, to allow room for adjustments at other stages. In general,

intentional contraventions will attract a higher percentage rate than negligent contraventions. This determines the maximum financial penalty considered by the Commission in a given case (**"Case Max FP"**).

98 Once the Case Max FP is determined, the Commission will proceed to apply the five-step methodology of the FP Framework to quantify the appropriate financial penalty for each case.

Step 1 – Identifying the level of culpability and harm

99 First, the Commission will identify the level of culpability and harm of the non-compliance.

100 Considering all the relevant factors, the Commission will determine whether the level of culpability is **"low"**, **"medium"** or **"high"**. Some of the factors that go towards the Commission's assessment of the level of culpability include (but are not limited to):

(a) The nature, gravity and duration of the organisation's non-compliance[37];

(b) If the organisation's contravention was negligent, the extent of the negligence; and

[37] Section 48J(6)(a) of the PDPA.

(c) If the organisation's contravention was intentional, factors including the degree of planning and pre-meditation[38].

101 Considering all the relevant factors, the Commission will determine whether the level of harm is **"slight"**, **"moderate"** or **"severe"**. Some of the factors that go towards the Commission's assessment of the level of harm include (but are not limited to):

(a) The type, nature and/or sensitivity of the personal data affected[39];

(b) The gravity of the organisation's non-compliance[40], for example the number of affected individuals;

(c) The extent of harm or prejudice caused to individuals (if any) as a result of the non-compliance, for example unauthorised disclosure of personal data which could expose individuals to greater risks of identity theft[41];

[38] *Neo Yong Xiang (trading as Yoshi Mobile)* [2021] SGPDPC 12 at [18].
[39] Section 48J(6)(b) of the PDPA.
[40] Section 48J(6)(a) of the PDPA.
[41] *KTT* at [38].

(d) The extent of risks the affected personal data was exposed to as a result of the non-compliance, for example, whether the affected personal data was only accessed, or whether it was publicly disclosed.

Step 2 – Calculating the Starting FP

102 Based on the level of culpability and harm assessed in Step 1, the Commission will identify the indicative levels of culpability and harm to determine the starting range and within that range, the approximate starting financial penalty to be imposed (**"Starting FP"**), up to the Case Max FP.

Step 3: Aggravating and mitigating factors

103 The Commission will then adjust the Starting FP to account for relevant aggravating and mitigating factors.

104 The relevant mitigating factors that the Commission may consider include (but are not limited to):

(a) where the organisation voluntarily takes timely and effective action to mitigate the effects and consequences of its non-compliance[42];

[42] Section 48J(6)(d) of the PDPA.

(b) where the organisation cooperates with the Commission's investigations[43];

(c) where the organisation voluntarily admits to its non-compliance (including by way of the Commission's Expedited Decision Procedure)[44];

(d) where the organisation has, despite its non-compliance, otherwise implemented adequate and appropriate measures for compliance with the PDPA[45]; and

(e) where the organisation has complied with any direction given by the Commission under section 48I or 48L(4) of the PDPA in relation to remedying or mitigating the effect of the non-compliance[46].

105 The relevant aggravating factors that the Commission may consider include (but are not limited to):

(a) where the organisation has previously failed to comply with the PDPA[47];

[43] *PPLingo* at [41(d)], Section 48J(6)(j) of the PDPA.
[44] *KTT* at [35(b)].
[45] Section 48J(6)(e) of the PDPA.
[46] Section 48J(6)(g) of the PDPA.
[47] Section 48J(6)(f) of the PDPA.

(b) Whether the organisation gained any financial benefit or avoided any financial loss as a result of the non-compliance[48];

(c) where the organisation has acted in a dilatory or uncooperative manner during the Commission's investigations[49]; and

(d) where the organisation fails to comply with any direction issued by the Commission under section 48I or 48L(4) in relation to remedying or mitigating the effect of its non-compliance[50].

Step 4: Impact of the financial penalty on the organisation

106 In Step 4, the Commission will determine whether the imposition of the proposed financial penalty will affect the organisation's ability to continue its usual activities[51]. This is a question of assessing the likely impact of the financial penalty on the financial health of the organisation and will be based on the available evidence,

[48] Section 48J(6)(c) of the PDPA.
[49] *Eatigo* at [21] and [27].
[50] Section 48J(6)(g) of the PDPA.
[51] Section 48J(6)(i) of the PDPA.

including from the representations furnished by the organisation. The financial penalty should not impose a crushing burden or cause undue hardship to the organisation[52].

107 If the Commission assesses that the financial penalty would adversely affect the organisation's ability to continue its usual activities, the Commission may (i) extend the time for payment of the financial penalty, (ii) allow for payment of the financial penalty to be made in instalments, or (iii) reduce the amount of the financial penalty.

Step 5 – Final adjustment

108 Finally, the Commission will take a "last look" at the amount of the financial penalty derived via Steps 1 to 4, and make any final adjustment to ensure that the proposed financial penalty is effective and proportionate[53]. This does not constitute a *carte blanche* to wholly revise the derived financial penalty. In most cases, the Commission expects that all relevant considerations would have been taken into account as part of Steps 1 to 4. Step 5 merely provides the Commission with a final opportunity to consider whether the amount of the financial penalty strikes the appropriate balance between achieving effective deterrence and ensuring proportionality.

[52] *Re Jigyasa* [2021] SGPDPCR 1; *Commeasure Pte Ltd* [2021] SGPDPC 11; *Neo Yong Xiang (trading as Yoshi Mobile)* [2021] SGPDPC 12.
[53] Section 48J(6)(h) of the PDPA.

Application of FP Framework to the present case

109 The Commission now explains how the FP Framework was applied to determine the appropriate financial penalty to be imposed on the Organisation for its negligent breach of the Protection Obligation, and also address the representations made by the Organisation relating to the preliminary financial penalty.

Preliminary Step – Determining the Case Max FP

110 Since the Organisation is in the High Turnover Class, the applicable **Statutory Maximum FP is 10% of the Organisation's annual turnover**. Based on the nature of the Organisation's **negligent** contravention of the Protection Obligation, the Commission applied the appropriate percentage rate subject to the quantum cap, which is below the Statutory Max FP, to derive the Case Max FP.

Step 1 – Identifying the level of culpability and harm

111 Based on the nature, gravity and duration of the Organisation's contravention of the Protection Obligation, the Commission determined the Organisation's level of culpability to be **low**.

112 Based on the fact that the Incident led to the unauthorised access to, and exfiltration of the personal data of 665,495 individuals but that the Affected Data only comprised the names, email addresses, phone numbers, countries of residence and SRL membership information of the affected individuals, the Commission determined the level of harm to be **moderate**.

Step 2 – Calculating the Starting FP

113 Based on the specific factors relevant to culpability and harm as assessed in Step 1, the Commission determined the starting range and approximate starting financial penalty within the low-moderate band.

Step 3 – Mitigating and aggravating factors

114 In the preliminary decision, the Commission had taken into account the mitigating factors set out at [30] in applying a reduction to the Starting FP.

115 In its representations on the Commission's preliminary decision, the Organisation contended that the Commission had not taken into account two additional mitigating factors which warranted a further reduction in the financial penalty:

(a) This was the Organisation's first instance of non-compliance with the PDPA; and

(b) The Organisation had voluntarily notified all individuals affected by the Incident in a reasonably timely manner, going beyond its legal obligation under section 26D(2) of the PDPA.

116 On (a), the fact that this was the Organisation's first non-compliance with the PDPA is merely a neutral factor, and not a relevant factor which merited further reduction of the financial penalty. In the Commission's decision in *Redmart Limited* [2022] SGPDPC 8, the organisation argued that a further reduction in the financial