**PERSONAL DATA PROTECTION COMMISSION**

Case No. DP-2305-C1061

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

And

Goldheart Jewelry Pte. Ltd.

… *Organisation*

---

# DECISION

---

# Goldheart Jewelry Pte. Ltd.

# [2025] SGPDPC 4

Lew Chuen Hong, Commissioner — Case No. DP-2305-C1061

20 June 2025

## Introduction

1 The Organisation is in the business of retail sale of jewellery through an online store ("**Website**") and through its physical outlets in Singapore. The Organisation is majority owned and controlled by Aspial Corporation Limited ("**Aspial**"). In this decision, Aspial Group refers to Aspial and its subsidiaries, including the Organisation.

2 On 26 May 2023, the Organisation notified the Personal Data Protection Commission (the "**Commission**") of a data breach incident involving the unauthorised disclosure of the personal data of 41,379 individuals using the Organisation's Website (the "**Incident**").

3 The Commission commenced investigations to determine the Organisation's compliance with the Personal Data Protection Act 2012 ("**PDPA**") in relation to the Incident. On 28 February 2024, the Organisation requested for the investigations into the Incident to be handled under the Commission's Expedited Decision Procedure ("**EDP**"), which the Commission acceded to. To this end, the Organisation voluntarily and unequivocally admitted to the facts set out in this decision and to its contravention of Section 24 of the PDPA in respect of the Incident.

## Facts of the Case

4 The Organisation's Website was built on an open-sourced e-commerce platform known as "Magento". The Organisation possesses the personal data of its customers, which is stored on a database management system hosted on its web server, known as "MariaDB". The Organisation had engaged a vendor (the "**Vendor**") to provide maintenance services for its Website. Pursuant to the terms of the Organisation's service agreement with the Vendor ("**Service Agreement**"), the Vendor provided maintenance services, including applying security patches to the Website, upon the Organisation's request. For completeness, the Vendor was not the Organisation's data intermediary in relation to the majority of the services provided under the Service Agreement as it did not process any personal data apart from the incidental processing of data whilst providing maintenance services for the Website.

5 The Organisation was required to adhere to the Aspial Group's Patch Management Policy ("**PMP**"), which provided an overall strategy to implement patch management processes of all the organisations under the Aspial Group. Based on the PMP, Aspial Group's IT infrastructure team was responsible for, amongst other things, (i) patch management, including monitoring new patch releases relating to all system platforms and software used; and (ii) informing vendors who manage external applications of security vulnerabilities, and requesting the vendors to validate and update the applications if required.

*The Incident*

6 On 24 May 2023, the Organisation was made aware that its customer database, including the personal data of its customers, had been published to an online forum by an unidentified threat actor ("**TA**").

7 The Organisation engaged cybersecurity service providers ("**Consultant**") to conduct forensics investigations on the Incident.

8 The Consultant found that the Incident arose from a delay in implementing a patch on Magento. On 13 February 2022, a patch was made available for the Magento platform, to address a common vulnerability and exposure known as CVE-2022-24086. CVE-2022-24086 was a security vulnerability which, if exploited, allowed a threat actor to execute codes remotely. However, the patch was not applied on the Organisation's Website until January 2023, 11 months after the patch was made available. It was further observed that plaintext credentials had been stored within the web server environment. This may allow a bad actor to leverage these credentials to gain unauthorised access within the server.

9 While the Website remained exposed to the vulnerability, the TA exploited CVE-2022-24086 to deploy malicious files onto the Website's server. The TA gained access to, and exfiltrated the data stored in MariaDB, and published the database on an online forum on or around 19 May 2023 ("**Affected Database**").

10 The Affected Database contained the following personal data:

| **Number of affected individuals** | Customers' data |
|---|---|

| | |
|---|---|
| **Types of personal data** | i. Name;<br>ii. Email Address;<br>iii. Date of Birth;<br>iv. Contact Number (approximately 3,500 individuals affected);<br>v. Billing Address (approximately 3,500 individuals affected); and<br>vi. Shipping Address (approximately 3,400 individuals affected). |

*Remedial actions*

11 Following the Incident, the Organisation implemented the following remedial measures:

Actions to mitigate the effects of the Incident

(a) Suspended the Website upon discovering the Incident.

(b) Removed the malicious files and plaintext credentials that were found in the Website's server.

Actions to prevent recurrence of the Incident or similar incidents

(c) Reset the password of the web server's underlying operating system's passwords.

(d) Reviewed and removed the operating system accounts which were not needed.

(e) Generated new SSH[1] keys for the web server and replaced existing SSH keys for each applicable operating system user.

(f) Reset all administrator passwords and implemented access control measures such as multi-factor authentication (MFA) when logging into administrative portal and limiting users' access based on their roles.

(g) Reviewed the security settings in the administrative backend by the Vendor, and set the security settings in accordance with Adobe's recommendations.

(h) Applied security patches and upgrades to Magento to the latest version.

(i) Ensured that the server hosting the Website is equipped with monitoring and detection tools.

## Findings and Basis for Determination

*The Protection Obligation under section 24 of the PDPA*

12 Based on the circumstances of the Incident, 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**

[1] Secure Socket Shell (SSH), also known as simply Secure Shell, is a cryptographic protocol, primarily used to enable secure access to remote servers and devices over the internet. It operates on public key cryptography that provides a mechanism for mutual authentication between the server and the client and establishes an encrypted channel of communication between them over an unsecured network.

**Obligation**”). The Organisation was determined to have breached the Protection Obligation in two respects.

*Failure to implement adequate patch management processes*

13 In implementing cybersecurity arrangements to safeguard personal data, it is common for organisations to rely on vendors to carry out cybersecurity practices such as patching. The Commission recognises that some organisations may lack the technical knowledge or resources to ensure that their systems are kept updated and patched, and therefore depend on third party vendors to assist in this regard.

14 The above practice does not absolve an organisation from being accountable for how it manages its vendors. The Commission has consistently emphasised that organisations need to elucidate their vendors’ cybersecurity responsibilities in its contracts with its vendors.

15 In *Re Civil Service Club* [2020] SGPDPC 15, the Commission opined at [14]:

> “In the circumstances, and in order for the Organisation to comply with the Protection Obligation, the Organisation should have ensured that it provided sufficient clarity and specifications on requirements to the Vendor (when developing and troubleshooting the CMS, Membership Portal and Virtual Cards) to protect the Members Data…. [T]he Organisation could have reviewed the Contract to include clauses setting out requirements for the Vendor to protect the Members Data.”

16 In *Re Smiling Orchid (S) Pte Ltd* [2016] SGPDPC 19*,* the Commission stated at [51]:

> “Data controllers that engaged outsourced service providers have to be clear about the nature and extent of services that the service provider is to provide. There must be a clear meeting of minds as to the services that the service provider has agreed to undertake, and this should be properly documented. Data controllers should follow through with the procedures to check that the outsourced provider is indeed delivering the services. In the absence of such clarity of intent and procedures, it is risky to hold that the outsourced service provider is a data intermediary.”

17 The Commission gave guidance in its Guide to Data Protection Practices for ICT Systems[2]: “Ensure that outsourced IT vendors are aware that the organisation intends to use their services to handle personal data, and they are clear on their responsibilities and requirements for data processing.”

18 Absent such clear provisions setting out the clear allocation of responsibilities, the obligation to implement the applicable security arrangement falls squarely on the organisation.

19 In the present case, based on how the contractual arrangements between the Organisation and Vendor allocated the parties’ respective cybersecurity responsibilities, the Commission did not consider it reasonable for the Organisation to rely entirely on the Vendor to monitor and apply software upgrades and patches. In its responses to the Organisation, the Organisation claims to have outsourced its patch management process to the Vendor. This is incongruent with the Service Agreement and the PMP, which stipulate that the Organisation is responsible for patch monitoring

[2] https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/other-guides/tech-omnibus/guide-to-data-protection-practices-for-ict-systems.pdf

and for requesting its Vendor to apply patches when necessary. The Vendor acts only upon the Organisation's request.

20 The Organisation did not monitor for nor request its Vendor to apply the patch apply for CVE-2022-24086, despite it being a known vulnerability. The Organisation also made no effort to regularly monitor for updates or patches, save for requesting for the Vendor to perform a scan using the Magento Security Scanner on 8 December 2022. However, this scan was inadequate in detecting the abnormalities within the server.

21 The Organisation should have put in place processes to monitor upgrades and patches, and to request that its Vendor perform upgrades and apply patches pursuant to the Service Agreement where necessary.

*Failure to implement reasonable access controls*

22 When developing access control measures for their network, an organisation should implement reasonable security arrangements to limit access to data and information contained therein. This includes restricting access to data capable of facilitating further access to other parts of an organisation's network. In *Re Redmart Limited* [2022] SGPDPC 8 ("**Redmart**"), the Commission found the organisation in breach of the Protection Obligation when it stored its API keys in source code and plain text in GitHub repositories and an Amazon Web Services private S3 bucket.[3] This allowed too many accounts to access them, and allowed the TA to access the keys after he gained access to the GitHub repositories and AWS environment.

[3] API refers to application programming interfaces. S3 refers to Simple Storage Service.

23 In the present case, it appeared that the Organisation failed to implement reasonable access controls in relation to the plaintext credentials that were stored in the server. Credentials were stored in plaintext on the Website's server without encryption or password protection.

24 The Organisation claimed that the plaintext credentials were left on the web server by its Vendor, and that it had no knowledge of its presence until alerted to it by the Consultant. The Commission emphasises that engagement of a third-party vendor does not absolve an organisation of its responsibility to protect personal data within its possession or under its control. Organisations are ultimately responsible for ensuring that there are reasonable security arrangements in place, including implementing reasonable access controls.[4].

25 The Commission reiterates the following in *Re WTS Automotive Services Pte. Ltd.* [2018] SGPDPC 26 ("***Re WTS Automotive Services***") at [23]: "…while [organisations] may delegate work to vendors to comply with the PDPA, the organisations' responsibility for complying with statutory obligations under the PDPA may not be delegated."[5]

26 In this case, the Organisation had merely relied on the Vendor to maintain the Website, without proper oversight of the Vendor. The Organisation should have monitored its Vendor when implementing access control measures, or conducted its own regular reviews to ensure that reasonable controls are in place.

27 The Commission stated in *Re WTS Automotive Services*, at [18]:

[4] See *Re Smiling Orchard (S) Pte Ltd and Ors* [2016] SGPDPC 19 at [46].

[5] See also *Re Singapore Health Services Pte. Ltd. & others [2019] SGPDPC 3*, at [56]

> "The Commission also recognises that "personal data of individuals may be exposed if the website or database in which it is stored contains vulnerabilities. There needs to be a regular review to ensure that the website collecting personal data and the electronic database storing the personal data has reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks". The Commission considers that it is good practice for an organisation to "conduct regular ICT security audits, scans and tests to detect vulnerabilities"."

28 For the above reasons, the Organisation is found to have negligently breached the Protection Obligation by (i) failing to implement adequate patch management processes; and (ii) failing to implement reasonable access controls in respect of the plaintext credentials stored on the Website's server.

**The Commissioner's Decision**

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

30 The Commission considered that in terms of the nature, gravity and duration of the non-compliance by the Organisation, the Organisation's breach of the Protection Obligation stemmed from its failure to contractually provide for its vendors' obligations as intended, and failing to monitor and request its Vendor to apply the patch for known vulnerabilities. The Commission notes that the known vulnerability CVE-2022-24086 remained unpatched for at least 11 months.

31 Further, the plaintext credentials were kept in the Website's server wholly unnoticed by the Organisation. In addition, personal data was exfiltrated and the threat actor published the personal data of the affected individuals on an online forum.

32 In terms of the type and nature of the personal data affected by the non-compliance by the Organisation, the Organisation's breach of the Protection Obligation led to the unauthorised access and disclosure of personal data of 41,379 individuals. The Commissioner notes that the affected personal data included names, dates of birth and basic contact information.

33 The Commission considered that at the time of the Incident, the Organisation had appointed a data protection officer and had data protection policies in place. The Organisation had deployed security measures such as deploying end-point security to scan all software and data files and deploying anti-virus software. The Organisation also requested its Vendor to perform scans using the Magento Security Scanner, the last scan of which was on 8 December 2022.

34 In addition, in order to ensure that the financial penalty imposed is proportionate and effective, having regard to achieving compliance and deterring non-compliance with the PDPA, the Commission also considered the Organisation's turnover together with the factors set out above, in particular the culpability of the Organisation and the harm caused to individuals, to determine the appropriate starting point for the financial penalty to impose on the Organisation.[6]

[6] See *Re Keppel Telecommunications & Transportation Ltd [2024] SGPDPC 3* at [40], *Re Fullerton Healthcare Group Pte Ltd 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]

35 Thereafter, the Commission took into consideration the following factors which warranted a reduction to the starting point for the financial penalty:

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

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

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

36 Finally, the Commission also considered if the financial penalty would be proportionate and effective as a deterrent to ensure compliance and deter non-compliance with the PDPA.

37 Based on the above assessment, the Commission preliminarily determined that a financial penalty of $64,000 should be imposed on the Organisation.

*Direction*

38 Separately, the Commission also took into account the following factors when deciding to direct the Organisation to carry out certain remedial measures under section 48I of the PDPA:

(a) Prior to the Incident, the Organisation had deployed security measures such as deploying end-point security to scan all software and data files and deploying anti-virus software.

(b) The Organisation also requested its Vendor to perform scans using the Magento Security Scanner, the last scan of which was on 8 December 2022. However, this failed to detect the vulnerability as described above, and was insufficient for the purposes of protecting a web server hosting customers' personal data.

(c) There was no regular extensive security testing and/or penetration testing performed on the Website's server. The security scans previously performed lacked proper patching and vulnerability management, given that the patch released on 13 February 2022 was only applied in January 2023. These were major factors that led to the Incident.

(d) The Organisation's existing security measures contained gaps in relation to access control measures and log retention policy.

(e) While the Organisation has taken steps to implement its remediation plan, the Commission views that the proposed remediation plan is insufficient to address all the deficiencies described above. A further audit and review is necessary to identify additional remediation measures.

## Representations made by the Organisation

39 The Organisation was notified of the preliminary decision by way of the Commission's letter dated 30 October 2024 and was invited to make representations. On 22 November 2024, the Organisation made representations to the Commission seeking a reduction in the financial penalty.

*Representations that the Vendor was the Organisation's data intermediary*

40 The Organisation submitted that its Vendor was its data intermediary, and that the Vendor had control and management of the MariaDB database at all times.

41 The Commission does not accept that the Vendor was the Organisation's data intermediary. A data intermediary is an organisation which processes personal data on behalf of another organisation. The Vendor's scope of work under the Agreement did not include processing of personal data. Under the Agreement, the Vendor was responsible for "backend programming and database configuration". Based on its investigations, the Commission is satisfied that this did not involve the processing of the Organisation's personal data, and is confined to adjustment of settings and optimisation of performance of the database, and such service was provided based on the Organisation's request and specifications. Where the Vendor carried out some incidental processing of personal data in relation to database configuration, this does not extend to being responsible for security arrangements surrounding personal data, which remains with the Organisation.

42 The Organisation submitted that its Vendor had retrieved a list of compromised personal data from the database, and had removed "spam" entries in the database. While this is data processing, this was done at the request of the Organisation post-Incident, and not relevant to the question of whether the Vendor was the Organisation's data intermediary at the time of the Incident.

43 In any event, even if the Organisation did engage a data intermediary, it was not absolved of its responsibilities to take steps to protect the personal data in its possession or under its control. Data controllers are not entitled to wash its hands

clean of its responsibilities under the PDPA. This will be addressed further in the next representation,

*Representations on the Vendor's responsibility to apply security patches*

44 The Organisation submitted that the Vendor had acted on their own initiative when it came to applying security patches and scanning of vulnerabilities. The Organisation therefore considered it the Vendor's obligation to monitor patch releases and apply them. Further, the Organisation stated that since the Vendor was the Organisation's data intermediary and a service provider specialising in Magento, it was inconceivable for the Vendor to not monitor patch releases or remain idle and await the Organisation's requests before patching.

45 The Commission does not accept the Organisation's representations. As explained in at paragraphs [40] to [42] above, the Commission does not consider the Vendor to be the Organisation's data intermediary. The fact that its Vendor applied some security patches on their own initiative does not assist the Organisation, as the Service Agreement clearly stated that patching was to be done upon the Organisation's request. The obligation remains with the Organisation to implement security arrangements, including clearly setting out its vendors' cybersecurity responsibilities in its contracts. The Vendor's actions do not cure the Organisation's failure to stipulate the parties' respective security responsibilities clearly in their contractual arrangements.

46 The Organisation submits that there was a "dearth of information regarding the application of Magento security patch APSB22-12 in particular, it is possible that [the Vendor] could have acted on their own initiative to apply the patch in January 2023

without receiving any request OR that a request was actually made". This is mere speculation that the Commission cannot give credence to, and illustrates precisely the shortcomings of the Organisation in failing to implement adequate patch management processes, and instead relying on the initiative of its Vendor.

*Representations relating to previous decisions*

47 The Organisation cited seven previous decisions by the Commission in support of its representations that the intended financial penalty ($64,000) was excessive for similar or more serious breaches of the PDPA. The Organisation's representations are not accepted as the factors considered in each case differed from the present case.

48 The cases cited are as follows:

(a) Cortina Watch Pte Ltd [2024] SGPDPCS 3 ("*Cortina Watch*"), where the Commission issued directions to the organisation, and did not impose a financial penalty.

(b) The Law Society of Singapore [2023] PDPC 4 ("*The Law Society*"), where the Commission issued directions to the organisation, and did not impose a financial penalty.

(c) FortyTwo Pte Ltd [2023] SGPDPCS 3 ("*FortyTwo*"), where sensitive personal data such as credit card details was affected, and where the Commission imposed a financial penalty of $8,000 on the organisation.

(d) Horizon Fast Ferry Pte Ltd [2024] SGPDPC 1, where the personal data of 108,488 was affected, and where the Commission imposed a financial penalty of $28,000 on the organisation.

(e) Consumers' Association of Singapore (CASE) [2024] SGPDPC 4, where affected individuals had suffered monetary losses, and where the Commission imposed a financial penalty of $20,000 on the organisation.

(f) Ascentis Pte Ltd [2023] SGPDPC 10, where the Commission imposed a financial penalty of $10,000 on the organisation.

(g) Commeasure Pte Ltd [2021] SGPDPC 11, in which the personal data of 5,892,843 individuals was affected, and where the Commission imposed a financial penalty of $74,000.

49 The Commission takes into consideration an organisation's turnover in determining the financial penalty imposed (see [34] above). For this reason, the financial penalty imposed against one organisation may differ from another even if there are other similarities in the breaches committed, where the turnovers of the organisations are different. The Commission opined in *Re Keppel Telecommunications & Transportation Ltd* [2024] SGPDPC 3 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 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."

50 The nature, gravity and duration of an organisation's non-compliance are also taken into account in determining the financial penalty. For instance, in the present case, the impact of the data breach was higher than *Cortina Watch* and *FortyTwo*, where the number of affected individuals were much lower (3,953 and 6,241 respectively).

51 In addition, the decision in *The Law Society* can be further distinguished. There, the Commission found the Organisation to be reasonable in relying on its vendor to perform security patching, and did not find breach of the Protection Obligation. This was because the Commission found there to be adequate processes to monitor and oversee the vendor:

> "20 The Commission appreciates that the technical nature of information on software patching and upgrades limits the degree of oversight that many organisations can exercise on vendor performance in this regard. The Commission notes that the Organisation had put in place a process to ensure that there were maintenance logs in respect of the Vendor's activities. Thus, the Organisation, to its credit, had put in place a system to monitor its Vendor's activities. In technical areas where the Organisation depends on its Vendor's technical expertise, this is reasonably adequate."

52 In contrast, the Organisation relied entirely on its Vendor to conduct patching, without having put in place any process to monitor or manage it.

*Representations on the storing of plaintext credentials*

53 In the preliminary decision, the Commission had found at paragraphs [22] to [24] above that, part of the Organisation's non-compliance with the Protection Obligation related to storing plaintext credentials in its web server. The Organisation submitted that it was not reasonable to expect it to locate or be aware of the plaintext credentials stored in the web server. It was the Organisation's Vendor that had the necessary expertise and legitimate access to the web server. Therefore, the Organisation had expected its Vendor to have taken adequate measures to protect sensitive credentials. To substantiate this, the Organisation provided the Commission with the Vendor's email confirmation that "the plaintext credentials were necessary for services to operate and were stored in a secure environment with appropriate permissions in place".

54 Upon receipt of the new information in the Organisation's representations, the Commission carried out its own line of enquiry with the Vendor, to ascertain (1) whether the storing of the plaintext credentials in such a manner was indeed necessary; (2) and if so, whether adequate security measures had been implemented to mitigate its risk. Following this inquiry, the Commission was satisfied that the plaintext credentials were necessary configuration files for the operation of the Magento platform. While no passwords or encryption controls were applied as noted above, the Vendor was able to show that reasonable access controls were implemented to restrict unauthorised access to these files, aligning with data

protection best practices.[7] The Commission also considered that there had been no conclusive evidence that the TA had exploited the plaintext credentials to access the personal data. As such, the Commission accepts the Organisation's representations in respect of the plaintext credentials.

55 Having considered all the relevant factors in this case, the Commission hereby requires the Organisation to pay a financial penalty of $58,000 within 30 days from the date of the directions, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

56 Having considered all the relevant factors of this case, the Commission also directs the Organisation to carry out the following within 60 days:

(a) Engage a third-party cyber security vendor to conduct a targeted security audit to enhance access control to personal data in the Organisation's possession within its network;

(b) Rectify any security gaps identified in the security audit; and

(c) Furnish to the Commission a report of the above security audit and rectification actions within 7 days of its completion.

**WONG HUIWEN DENISE**
**DEPUTY COMMISSIONER**
**FOR COMMISSIONER FOR PERSONAL DATA PROTECTION**

[7] See pages 15 to 16 on "Authentication, authorisation and passwords" in the Commission's Guide to Data Protection Practices for ICT Systems.