PERSONAL DATA PROTECTION COMMISSION

[2021] SGPDPCR 1

Case No. DP-1707-B0922

In the matter of a reconsideration application under section 31(1)(b) of the Personal Data Protection Act 2012

And

Jigyasa

… *Organisation*

RECONSIDERATION DECISION

Data Protection *– Protection obligation – Unauthorised disclosure of personal data – Insufficient security arrangements*

Data Protection *– Accountability obligation – Lack of data protection policies and practices*

Data Protection *– Accountability obligation – Failure to appoint data protection officer*

Re Jigyasa

[2021] SGPDPCR 1

Lew Chuen Hong, Commissioner — Case No. DP-1707-B0922

29 January 2021

Background and Application for Reconsideration

1 In *Re Jigyasa* [2020] SGPDPC 9 (the "**Decision**"), Jigyasa (the "**Organisation**") was found to be in breach of section 24 of the Personal Data Protection Act 2012 (the "**PDPA**"). The grounds of decision and the full facts of the case are set out in the Decision.

2 Briefly:

(a) there was risk of unauthorised access and disclosure of employee assessment reports, such as 360 Feedback Reports and evaluation reports (collectively, the "**Reports**") relating to 671 employees of the Organisation's clients ("**Affected Individuals**"), on the Organisation's website ("**Website**").

(b) The Reports were generated based on survey results collected by the Organisation via its web application (the "**Web Application**") and

stored in a folder on the server which hosted the Web Application[1] ("**the Server**"). The Organisation discontinued use of this Web Application in 2010[2].

(c) On 10 July 2017, Reports concerning 3 of the Affected Individuals were discovered to be publicly accessible from links generated by Internet searches ("**the Incident**")[3].

(d) In the course of investigations by the Commission, the Organisation was unable to provide a clear account on what led to the Incident, and did not appear to be familiar with the security arrangements of its Website. In particular, the Organisation did not appear to know that a request for a 360 Feedback Report via the Web Application resulted in a copy of the Report being saved on the Server[4].

(e) The Commission accepted that the webpages containing the Reports may have been inadvertently created on or around February 2017 when the Organisation's Website was being redesigned by an independent developer ("**the Developer**")[5].

(f) The Organisation did not give any specific instructions to the Developer to protect personal data or on security arrangements of its Website during the redesign process, and relied solely on the goodwill and integrity of the Developer to conduct the redesign properly, without

---

[1] Paragraph 2 of the Decision

[2] Paragraph 5 of the Decision

[3] Paragraph 3 of the Decision

[4] Paragraph 5 of the Decision

[5] Paragraph 6 of the Decision

any documentation, supervision or other means of control[6]. The Organisation mistakenly believed that the Reports and their contents had been removed from the Server when the previous Website was discontinued[7].

(g) The Organisation also failed to conduct vulnerability scans or any other form of security testing for the Website prior to the redesigned Website going live, or anytime afterwards[8].

(h) In addition, the Organisation did not appoint a data protection officer ("**DPO**") or develop and implement any data protection policies[9].

3 The Organisation was found to have contravened sections 11(3), 12 and 24 of the PDPA, and directed to (i) pay a financial penalty of $90,000; (ii) appoint a DPO; and (iii) develop and implement policies and practices that are necessary for the Organisation to meet its obligations under the PDPA, and communicate them to its staff.

4 The Organisation submitted an application for the reconsideration of the Decision (the "**Application**") seeking a removal of the financial penalty imposed or, in the alternative, a reduction in the quantum of the financial penalty.[10]

---

[6] Paragraph 11 of the Decision

[7] Paragraph 10 of the Decision

[8] Paragraph 15 and 17 of the Decision

[9] Paragraphs 19 to 22 of the Decision

[10] Pursuant to Regulation 12(1) of the PDP (Enforcement) Regulations 2014, a copy of the Application was served on the three individuals who had complained to the Commission that when they searched their names on the Internet, the search results included links to copies of

(*cont'd on next page*)

The Organisation's Submissions

5 The key points raised by the Organisation in response to the Commission's findings and in support of its Application, are summarised below.

(a) In relation to the factual findings in the Decision:

(i) Contrary to the findings summarised at [2(d)], the Organisation had represented that it had provided a clear account on what led to the Incident during the course of the investigation. The Organisation also clarified that it was aware the Web Application was meant to generate the Reports.

(ii) With respect to the findings summarised at [2(f)], the Organisation clarified that it had discussed the scope of work with the Developer.

(iii) In relation to the findings summarised at [2(g)], the Organisation clarified that it had conducted vulnerability scans on the Website in April 2017 and 2019 in the form of penetration testing.

(b) The Organisation also sought to rely on the following factors in mitigation:

---

their 360 Feedback Reports, and these reports were accessible through the links. One complainant informed the Commission that he did not wish to pursue the matter, while the other two complainants did not respond.

(i) The links to the Reports were in the public domain for less than 5 months, and the majority of the links were accessed through internet bots;

(ii) While agreeing that the Reports should not have been exposed to the world at large, the Organisation pointed out that the feedback provider for the Reports was anonymous and the Reports were 7 years old. In the Organisation's view, feedback on an individual's current position would be more relevant and carry more weight than the Reports;

(iii) Out of the 671 Reports, 204 Reports belonged to one of the Organisation's clients based in India. The Organisation submitted that the 204 Reports ought to be taken as a mitigating factor in relation to the total number of Affected Individuals. This was because the Organisation's agreement with its client was based on the prevailing laws of India (i.e. where that client's business was registered) and India's data protection bill was only tabled in parliament in December 2019;

(iv) The fact that the Reports were exposed to the risk of unauthorised access and disclosure for more than 7 years (between 2009 to 2017) should not be considered an aggravating factor in paragraph 32(b) of the Decision. This was because the Organisation had retained the Reports for its long-term clients that required such historical and analytical data. The retention of the Reports was also in accordance with the Organisation's retention policy; and

(v) The Organisation has been in business for over 16 years, and the Incident was a "*one-off*" case caused by human error, not a systemic failure.

(c) With respect to the findings in relation to breach of section 11(3) of the PDPA, the Organisation explained that the sole proprietor understood that she would be "automatically" considered as the Data Protection Officer ("**DPO**"), and therefore did not formally appoint a DPO. This was because at the material time, the Organisation did not have any full-time employees, and its sole employee was only working part-time. In addition, the contact details on the Organisation's website directed parties to contact the sole proprietor.

(d) In addition, the Organisation also submitted that the financial penalty the Commissioner had intended to impose would put a crushing burden on the sole proprietor of the Organisation, as well as her family.

(i) The Organisation suffered losses due to the Covid-19 pandemic. In particular, the Organisation's only project for 2020 was suspended due to circuit breaker measures imposed by the Singapore government, and it remains unknown whether the project will resume;

(ii) The Organisation suffered financial losses as a consequence of the Incident due one of its clients cancelling contracts;

(iii) The sole proprietor did not have any income in 2019, and does not foresee any income in 2020; and

(iv) Notwithstanding the above, the Organisation has not retrenched its one employee, and the sole proprietor has been paying the employee's salary out of her own savings.

6 Separately, the Organisation also informed the Commission that it had complied with the Directions in the Decision to appoint a DPO, as well as to develop and implement policies and practices necessary for the Organisation to meet its obligations under the PDPA, and communicate them to its staff.

Findings and Basis for Determination

7 With respect to the Organisation's submissions in relation to the factual findings in the Decision at [5(a)], these are not mitigating factors that warrant a reduction in the financial penalty. In particular, when discussing the scope of work with the developer, the Organisation should have provided the Developer with clear and specific business requirements on the need for security arrangements for its Website to ensure that no personal data was exposed to risk of unauthorised disclosure or access as a result of the redesign. The Organisation did not do so. Further, the penetration tests conducted by the Organisation on its Website only took place after the redesigned Website went live. The Organisation should have conducted the vulnerability scans as a form of security testing on its Website prior to the redesigned Website going live.

8 The points raised by the Organisation at [5(b)] are not mitigating factors for the reasons explained below:

(a) The cause of the Incident was in fact the links being accessed by internet bots which led to the links being indexed and searchable on the Internet;

(b) The fact that the feedback providers were anonymous in the Reports and the fact that the Reports were 7 years old does not negate the potential harm to Affected Individuals;

(c) The Organisation's submission that the 204 Reports belonging to its client based in India ought to be taken as a mitigating factor in relation to the total number of affected individuals cannot be accepted. The PDPA protects personal data processed in Singapore with respect to all 671 Affected Individuals regardless of where they may have originated from;

(d) While the Organisation was required to retain the Reports for its long-term clients that required such historical and analytical data, this is not a mitigating factor that lowers the standard expected of the Organisation to implement reasonable security arrangements to protect the Reports from unauthorised access and disclosure. That said, given the Reports were retained at the Organisation's clients' request, the fact that the Reports were retained for over 7 years will not be treated as an aggravating factor; and

(e) The Incident revealed the Organisation's ignorance of the data protection provisions of the PDPA. The personal data in the Reports was sensitive in nature as they included data on the assessment of the affected individuals' work performance and unauthorised access of such data could potentially result in harm to the individuals concerned. The Commission's previous decisions have established that organisations are required to put in place more robust measures of protection for

personal data of a more sensitive nature.[11] Notwithstanding this, the Organisation omitted to conduct any security testing on its redesigned Website prior to launching it.

9 In relation to the Organisation's submissions at [5(c)] on the "automatic" appointment of sole proprietors as DPO, this may carry more weight in a scenario where the sole proprietor does not have any employees. In the present case, the Organisation had one employee. If there are employees, the law makes no assumptions as to who amongst them is the DPO. Crucially, organisations – including sole proprietors – may also appoint external professional DPOs with the requisite expertise and experience. For these reasons, a deliberate appointment is necessary.

10 The Organisation's financial circumstances and the sole proprietor's personal circumstances at [5(d)] were considered in mitigation. In particular, the exceptional challenges faced by businesses amid the current Covid-19 pandemic has been taken into account, bearing in mind that financial penalties imposed should not be crushing or cause undue hardship on organisations.

11 Having carefully considered the Application, and taking into account all the relevant facts and circumstances (including the Organisation's compliance with the Directions in the Decision at [6]), the Commissioner has decided to reduce the financial penalty imposed on the Organisation to $30,000 for the contravention of sections 11(3), 12 and 24 of the PDPA. Although a lower financial penalty has been imposed in this case, this is exceptional and should not be taken as setting any precedent for future cases.

---

[11] See for example, *Re Aviva Ltd* [2018] SGPDPC 4 at [16] to [17]

Conclusion

12 Given the foregoing, the Commissioner hereby varies the Directions in the Decision as follows: The Organisation is directed to pay a financial penalty of $30,000 within 30 days of the date of this Reconsideration Decision, 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.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION