PERSONAL DATA PROTECTION COMMISSION

[2020] SGPDPC 9

Case No DP-1707-B0922

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

And

Jigyasa

… Organisation

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*

Jigyasa

[2020] SGPDPC 9

Tan Kiat How, Commissioner — Case No DP-1707-B0922

30 March 2020

Introduction

1 This case concerns the unauthorised disclosure of employee assessment reports, such as 360 Feedback Reports and evaluation reports (collectively, the "**Reports**"), on the website ("**Website**") of Jigyasa (the **"Organisation**"), a human resource and management consultancy business.

Material Facts

2 The Organisation is a business operated by a sole proprietor with one part-time employee. 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. Reports documented 360 degree feedback on employees of the Organisation's clients, based on evaluation by their subordinates, supervisors and/or peers. The feedback included character qualities, for example whether they were considered fair, honest, reliable and trusted, demonstrated professional

behaviour at all times or had good technical knowledge. Each of these character qualities was given an average rating from a scale of 1 to 10, with 9-10 being an exceptional strength and 1-2 being below expectations. These Reports comprehensively set out such information for each named individual employee of the Organisation's clients. There is also a section which provides verbatim comments from respondents (e.g. "*handle more complex responsibilities*", "*slower support*"). Some of the Reports also included individual employees' qualities, such as leadership, integrity, decision-making, initiative, and professional disposition, ranked against their colleagues.

3 On 10 July 2017, the Personal Data Protection Commission (the "**Commission**") received complaints from 3 individuals (the "**Complainants**") alleging that when they searched their names on the Internet, the search results included links to copies of their 360 Feedback Reports, and these reports were accessible through the links (the "**Incident**").

4 When notifying the Commission, the Complainants stated that they expected these Reports to be private and confidential and that the disclosure of their 360 Degree Feedback Report would have a significant impact on their job prospects and career options. One of the Complainants alleged that as the industry the Complainant worked in is "*extremely niche*", "*this could be the reason [he has] not been successful in his job interviews over the past 2 years*". No evidence was adduced to support such claims. Nevertheless, the possibility that the information contained in the Reports may have been accessed by a prospective employer's human resource personnel as they conducted due diligence on job applications cannot be discounted.

5 The Organisation did not appear to be familiar with the security arrangements of its Website and was not able to provide clear accounts on what

led to the Incident during the course of the investigation. In this regard, it was noted that the Organisation had ceased the use of the Web Application in 2010, some 7 years before the Commission's investigation. The Organisation initially claimed that it did not know that when a client requested for a 360 Feedback Report using the Web Application, a copy of the Report would be saved on the Organisation's system as a PDF file. It claimed that the Report was dynamically generated by the Web Application and presented for viewing, without storing a copy on the Website. However, when the operation of the Web Application was demonstrated to it, the Organisation agreed that the Reports could have been created but disclaimed knowledge of this. It also maintained that the data should have been removed from the server when that particular version of the Web Application was discontinued in 2010. In this regard, the Organisation's explanation was that "*[the Web Application] and all its data should have been removed, but I am not sure if [the Web Application] is still in the server*".

6 In relation to how the Reports became publicly accessible, the Organisation's version of events is that the webpages containing the Reports (the "**Webpages**") were inadvertently created on or around February 2017 during the redesign of the Organisation's Website. The Organisation had engaged an independent developer (the "**Developer**") to redesign its Website by changing it from HTML to WordPress. The Developer provided a test URL to the Organisation to confirm that the Website was designed according to the latter's instructions. The Organisation did so, but did not detect that the Webpages had been created. According to the Organisation, during the redesign process, password protection for the Reports was not implemented even though this was implemented previously. On balance, the Organisation is given the benefit of doubt and its position that the Reports were made publicly accessible as a result of the redesign is accepted. The complaint to the Commission (on 10 July 2017), was submitted not long after the redesigning of the Website in or

around February 2017, and to the Commission's knowledge, there had not been any complaints prior to this. If the earlier version of the Website did not implement any form of access control, any one of the employees of the Organisation's clients who had used the system would likely have raised this as an issue and the Organisation would have had to rectify it.

7 At the time of the Incident, the webpages contained Reports relating to 671 employees of the Organisation's clients (the "**Affected Individuals**"). Depending on the type of Report, the information therein (collectively, "**Personal Data**") may have included:

(a) the names of the Affected Individuals;

(b) the name and addresses of the Affected Individuals' employers;

(c) appraisals of the Affected Individuals' work performance by subordinates, supervisors and/or peers;

(d) the Affected Individuals' 360 Feedback scores; and

(e) an indication of whether the Affected Individuals were top performers within their respective organisations.

Remedial Measures

8 Upon being notified of the Incident by the Commission, the Organisation undertook the following remedial actions:

(a) moved the Reports to password-protected locations and subsequently deleted Reports prepared for former clients;

(b) requested the service provider hosting the Website (the "**Webhost**") to provide the Organisation with the access logs for the Webpages;

(c) engaged a developer to scan the Website and find out whether there were more webpages containing Reports which were accessible through the Internet without any access restrictions; and

(d) requested the Webhost to conduct an audit of all web based applications and introduce enhanced security monitoring to prevent any lapses.

Findings and Basis for Determination

Whether the Organisation had breached section 24 of the PDPA

9 Section 24 of the Personal Data Protection Act 2012 ("**PDPA**") requires organisations to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Although the Organisation had engaged the Developer to redesign the Website, the Developer did not process any personal data on behalf of the Organisation. The Organisation managed the Website on its own and retained full responsibility for the IT security of the Website and the Personal Data.

10 First, as stated in paragraph 5 above, the Organisation demonstrated a lack of knowledge as to the security arrangements of its Website, in particular, the creation and storage of the Reports, and had been under the mistaken impression that the Personal Data had been removed from the server when the previous Website was discontinued. In order to fulfil its Protection Obligation,

the Organisation is required to, at the very least, be aware of how and where it stores personal data in order to implement measures to protect such data. In this regard, the *Guide on Building Websites for SMEs* (revised 10 July 2018) states that:

> "5.7 **Personal Data Inventory**
>
> 5.7.1 ***Organisations and any engaged IT vendors should keep track of where the collected personal data is stored***, and should impose a limit on how long the data is kept, or regularly review their need to continue storing the personal data.
>
> 5.7.2 If the personal data is no longer required, organisations and any engaged IT vendors should then ensure that the personal data is anonymised or disposed of in such a way that it cannot be recovered."
>
> [Emphasis added.]

11 Secondly, 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. The engagement was done over a short email exchange, and the Organisation could not produce the contract or evidence of any written instructions to the Developer on security arrangements. It had relied solely on the goodwill and integrity of the Developer to conduct the redesign properly, without any documentation, supervision or other means of control.

12 While the Organisation claimed that the Developer was engaged to merely change the "*look and feel*" of the Website, the facts suggest that the redesign of the Website was a more involved project which required a significant amount of coding work and amounted to building a new Website. In this regard, the Developer had expressly informed the Organisation that the

scope of work involved the need to redesign the Website on the WordPress environment instead of using the HTML coding of the existing Website and required the existing content on the Website to be migrated. This is not merely a redesign of the look-and-feel of the Website, but a redevelopment. Thus, the Organisation should have provided the Developer with clear instructions to ensure that no personal data was subject to unauthorised disclosure or access as a result of the redesign.

13 According to the *Guide on Building Websites for SMEs* (at [4.2]):

> "4.2.1 ***Organisations should emphasise the need for personal data protection to their IT vendors, by making it part of their contractual terms***. The contract should also state clearly the responsibilities of the IT vendor with respect to the PDPA. When discussing the scope of the outsourced work, organisations should ***consider whether the IT vendor's scope of work will include*** any of the following:
>
> - Requiring that IT vendors consider ***how the personal data should be handled as part of the design and layout of the website***.
>
> - Planning and developing the website in a way that ***ensures that it does not contain any web application vulnerabilities that could expose the personal data of individuals collected, stored or accessed via the website through the Internet***.
>
> …"
>
> [Emphasis added.]

14 The Commission has also taken a similar position in *Re Tutor City* [2019] SGPDPC 5, in which the organisation was unaware of its obligations under the PDPA and showed a lack of knowledge of the security arrangements

over its website. Specifically, the organisation in that case did not, *inter alia*, communicate any specific security requirements to its developer to protect the personal data stored on the website's server (including ensuring that the personal data would not be accessible to the public).

15 Thirdly, the Organisation failed to conduct vulnerability scans or any other form of security testing for the Website. As set out in the *Guide on Building Websites for SMEs* (at [5.6]):

> "5.6 **Security Testing**
>
> 5.6.1 ***Testing the website for security vulnerabilities is an important aspect of ensuring the security of the website***. ***Penetration testing or vulnerability assessments should be conducted prior to making the website accessible to the public, as well as on a periodical basis (e.g. annually).*** Any discovered vulnerabilities should be reviewed and promptly fixed to prevent data breaches.
>
> 5.6.2 ***Where organisations have outsourced the development of its website, they should either require the IT vendor(s) to conduct the above security testing, or arrange for a cybersecurity vendor to do so.*** As a baseline, organisations may wish to consider using the Open Web Application Security Project (OWASP) Testing Guide and the OWASP Application Security Verification Standard (ASVS) to verify that security requirements for the website have been met."
>
> [Emphasis added.]

16 In *Re InfoCorp Technologies Pte Ltd* [2019] SGPDPC 17, the Commission took the view that the organisation's failure to conduct web application vulnerability scans was a breach of section 24 of the PDPA, and that given the sensitivity of the personal data which the documents contained, it was

unreasonable that the organisation had omitted security testing prior to the launch of the website. Also, in *Re WTS Automotive Services Pte Ltd* [2018] SGPDPC 26, the Commission emphasised the need for regular review of security arrangements and tests to detect vulnerabilities, it stated (at [18]) that:

> "… [t]he 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***…"
>
> [Emphasis added.]

17 In this case, even if the Organisation was unaware that the Reports were being created and stored, had the Organisation conducted vulnerability scans as a form of security testing on its Website prior to the redesigned Website going live or at any time after that, the fact that the folders contained Reports with personal data and the fact that the Reports were publicly-accessible would likely have been detected and could have been remedied. As a result, the Organisation was unable to assess whether the folders ought to have been restricted. It also did not consider whether any webpages which were created as part of the redesign of its Website were correctly created.

18 The foregoing lapses demonstrate a fundamental lack of care by the Organisation over the personal data in its possession and/or under its control. It is clear that the Organisation had not applied its mind to its obligations under section 24 of the PDPA with respect to implementing adequate security

arrangements to protect the Reports. In view of the above, the Commissioner found the Organisation in breach of section 24 of the PDPA.

Whether the Organisation had breached sections 11(3) and 12 of the PDPA

19 Section 11(3) of the PDPA requires organisations to designate one or more individuals, typically referred to as the data protection officer ("**DPO**") to be responsible for ensuring the organisations' compliance with the PDPA. Section 12 of the PDPA requires organisations to, *inter alia*, develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA ("**Data Protection Policies**"), and to communicate information about such policies and practices to its staff.

20 In the course of the Commission's investigations, the Organisation admitted that it was unaware of the data protection provisions of the PDPA and was under the impression that the PDPA only relates to the Do-Not-Call provisions. Hence, the Organisation did not appoint a DPO or develop and implement any Data Protection Policies. In this regard, it is a trite principle of law that ignorance of the law is no excuse. Hence, the Organisation's lack of awareness of its obligations under the PDPA is not an excuse for contravening the PDPA.

21 The Organisation also admitted that, at the time of the Incident, it only had certain unwritten policies with respect to the protection of client data, which were communicated to its employees. In this regard, it is important to reiterate that an organisation's Data Protection Policies should be documented in a written policy, as per *Re Furnituremart.sg* [2017] SGPDPC 7 at [14]:

> "[t]he lack of a written policy is a big drawback to the protection of personal data. Without having a policy in writing, employees and staff would not have

> a reference for the Organisation's policies and practices which they are to follow in order to protect personal data. Such policies and practices would be ineffective if passed on by word of mouth, and indeed, the Organisation may run the risk of the policies and practices being passed on incorrectly. Having a written policy is conducive to the conduct of internal training, which is a necessary component of an internal data protection programme."

22 In light of the foregoing, the Commissioner found that the Organisation had also breached sections 11(3) and 12 of the PDPA.

Representations by the Organisation

23 In the course of settling this decision, the Organisation made representations on the amount of financial penalty that was to be imposed. The Organisation raised the following factors for consideration:

(a) The Commission should not have placed such significant weight on the Personal Data in the Reports that was exposed in the Incident. In this regard, the Personal Data in the Reports should not be accorded the status of sensitive personal data and treated as an aggravating factor because:

(i) The Reports did not contain the Affected Individual's identification/NRIC number, health data or biometric data. The identifying personal data was limited to the name of the Affected Individuals and the name of his/her employer; and

(ii) The feedback data in the Reports would not fall within the realm of what would typically be known as sensitive personal data as defined in Articles 9 and 10 of the European General Data Protection Regulation ("**GDPR**");

(b) Any aggravating weight to be given to the disclosure of the Reports must be reduced by the fact that evaluative purpose exception in the PDPA permits a prospective employer to obtain such feedback or evaluative information without consent of the Affected Individuals. The Organisation posited that the evaluative purpose exception tempers the extent of breach or application of the Protection Obligation because disclosure is permitted so long as the exception applies;

(c) The possibility of a member of the public specifically carrying out keyword searches of the names of Affected Individuals during the period when the specific URL links leading to the Reports had been exposed would not be high;

(d) The Reports were not more recent than the year 2010. As the Incident occurred in 2017, the accuracy of the contents of the Reports would have waned with the effluxion of time, and this could be a point taken into consideration by a prospective employer;

(e) In past decisions, the Commission has taken into consideration the financial circumstances of an organisation in determining the financial penalty (if any) to be imposed. The financial penalty that the Commissioner intended to impose would have a crushing burden on the Organisation, and cause undue hardship. Further, taking into consideration the type of personal data and the potential harm to the Affected Individuals, the proposed financial penalty would be disproportionately higher than what had been imposed on organisations in previous decisions; and

(f) The Incident was a one-off occurrence and there was no evidence that the Website was otherwise insecure. During the past 16 over years

that the Organisation has been in business, there were no other complaints in relation to unauthorised disclosure of personal data.

24 With respect to the Organisation's representations on the nature of the Personal Data in the Reports at [23(a)], Singapore's legislative approach to determining the sensitivity of personal data is different from jurisdictions like the European Union. Unlike the GDPR, the PDPA does not have a definition of sensitive personal data. It is inappropriate to draw comparisons with the GDPR approach to defining sensitivity of personal data as the jurisprudential basis of GDPR is markedly different from the PDPA. The Commission's approach in each case is to assess the nature of the personal data in question, taking into account specific circumstances such as the context in which the data was collected and the potential risk of harm due to unauthorised access or disclosure.

25 The Organisation's representations on the evaluative purpose exception at [23(b)] cannot be accepted. The fact that personal data that may be collected, used or disclosed under an exception to consent cannot *ipso facto* be equated with an inference that the class of personal data is less sensitive and need not be protected, or that there is less culpability for a failure to protect. It is necessary to examine the nature of the exception and the *raison d'etre* for its existence. The following analysis is confined to the evaluative purpose and is not intended to establish any special rule for personal data covered by other exceptions.

(a) The PDPA recognises that there is a class of personal data that exists for an evaluative purpose. A perusal of its definition discloses that the categories of activities are characterised by the need for full disclosure and frank discussions in order to arrive at a decision to, for example, employ, promote or dismiss a person, amongst a list of other

circumstances that circumscribe this purpose.[1] The recognition of the need for full disclosure and frank discussions is carried through in a number of exceptions, which permit personal data to be collected, used and disclosed without consent.[2] Further, personal data in the nature of opinion data kept solely for an evaluative purpose is exempted from the access and correction requirements.[3] The upshot of these exceptions is to recognise the necessity to preserve the space for full disclosure of relevant personal data and frank exchanges of views between persons who are tasked to conduct an evaluation before making a decision or recommendations leading to a decision.

(b) Given the nature of the evaluative purpose exceptions and their *raison d'etre*, it is necessary to ensure that organisations accord personal data that is covered by the evaluative purpose exceptions with a higher degree of protection. The *quid pro quo* for organisations having the liberty to collect, use and disclose personal data without consent for evaluative purposes, and to keep opinion data beyond the reach of data subjects for access and correction, is that they are expected to put in place more robust measures to comply with the Protection Obligation. In other words, personal data that is kept for an evaluative purpose should be treated as sensitive data and be protected to a greater degree.

---

[1] See definition of "evaluative purpose" in section 2 of the PDPA. See also Section 29(3) of New Zealand's Privacy Act 1993 which has a similar definition of "evaluative material" for the purposes of a refusal to disclose personal information pursuant to Principle 6 (Access to personal information).

[2] See para 1(f) of the Second Schedule, para 1(f) of the Third Schedule and para 1(h) of the Fourth Schedule of the PDPA.

[3] See para 1(a) of the Fifth Schedule and para 1(a) of the Sixth Schedule of the PDPA respectively. See also Section 29(1)(b) of New Zealand's Privacy Act 1993 which permits an agency to refuse to disclose personal information pursuant to Principle 6 if (i) the disclosure of the information or of information identifying the person who supplied it, being evaluative material, would breach an express or implied promise (i) which was made to the person who supplied the information; and (ii) which was to the effect that the information or the identity of the person who supplied it or both would be held in confidence.

(c) Further, the Incident in the present case involved the risk of unauthorised disclosure to the world at large whereas the evaluative purpose exception is much narrower in scope (i.e. it permits disclosure of personal data without consent to specific individual(s)/organisation(s) only where it is necessary for evaluative purposes). The expectations of persons who provided the 360-degree feedback would have been for their feedback to be accessed by persons with a role in evaluating the performance of the employee under review. It would be difficult, by any stretch of imagination, for them to accept that their feedback was accessible by the world at large.

26 The possibility of actual unauthorised disclosure raised by the Organisation at [23(c)] had already been taken into consideration in determining the financial penalty that was to be imposed. While the risk of actual unauthorised disclosure may have not been high, the fact that the Reports were exposed to the risk of unauthorised access and disclosure for more than 7 years (between 2009 to 2017) is particularly glaring.

27 As for the accuracy of the contents of the Reports at [23(d)], the passage of approximately 7 years is unlikely to make a significant difference to the potential harm suffered by the Affected Individuals due to unauthorised access or disclosure of the Reports, or dampen the expectations of the persons who provided feedback as discussed in [25(c)].

28 With respect to the Organisation's representations comparing the present case to earlier decisions at [23(e)], it needs only be said that each decision is based on the unique facts of that case. The decision in each case takes into consideration the specific facts of the case so as to ensure that the decision and direction(s) are fair and appropriate for that particular organisation.

29 The fact that the Incident may have been the Organisation's first data breach is not a mitigating factor. Conversely, if the Incident was a repeated contravention by the Organisation of the Protection Obligation, this would likely weigh in favour of a higher financial penalty.

30 Having carefully considered the representations, the Commissioner has decided to reduce the financial penalty to the amount set out at [33(a)]. The quantum of financial penalty has been determined after due consideration of the appropriate weight to be given to the aggravating factors at [32], the Organisation's financial circumstances and to avoid imposing a crushing burden on the Organisation. 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.

The Commissioner's Directions

31 In determining the directions to be imposed on the Organisation under section 29 of the PDPA, the Commissioner took into account, as a mitigating factor, the fact that the Organisation had promptly taken the remedial measures set out above (at [8]).

32 The Commissioner also took into account the following aggravating factors:

(a) the Personal Data in the Reports were 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 (for example, the individuals' future employment prospects may be affected);

(b) the Personal Data in the Reports was exposed to the risk of unauthorised access and disclosure for a period of more than 7 years; and

(c) the Organisation showed a lack of awareness of its obligations under the PDPA even though it processes large volumes of sensitive personal data in the course of its business.

33 Having carefully considered the facts and circumstances of this case and the above mitigating and aggravating, the Commissioner hereby directs the Organisation:

(a) To pay a financial penalty of $90,000 within 30 days of the date of this direction, 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;

(b) to appoint a DPO within 30 days from the date of this direction; and

(c) to 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, within 30 days of the date of this direction.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION