DECISION OF THE PERSONAL DATA PROTECTION COMMISSION

Case Number: DP-1611-B0319

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

And

Furnituremart.sg (UEN 53169430E)

… Organisation

Decision Citation: [2017] SGPDPC 7

GROUNDS OF DECISION

31 May 2017

1. This is a case involving an organisation which had issued to its customer (the Complainant) an invoice which had a separate invoice ("**second invoice**") containing personal data of another customer printed on the reverse side. In this regard, the other customer's personal data was disclosed to the Complainant, comprising of the following information of the other customer:

    a. Customer's surname;

    b. Home address;

    c. Delivery address;

    d. Telephone number; and

    e. E-mail address.

2. The Complainant made a complaint to the Personal Data Protection Commission (the "**Commission**") on 7 November 2016 of the disclosure that was made, and the Commission conducted an investigation into the matter. It now sets out its findings of its investigations below.

A. MATERIAL FACTS AND DOCUMENTS

3. The Organisation is in the business of trading furniture, bedding, and other domestic products.

4. Whenever it issues its invoices, the Organisation's procedure is to make three copies of every invoice: The first for the Organisation's filing, the second for the customer, and the third for the customer to sign and return to the Organisation on delivery of the goods.

5. According to the Organisation, all signed copies of invoices are supposed to be returned to its office, and subsequently destroyed by its staff on a daily basis.

6. In this case, however, the returned invoice was put in a printer feed tray, and re-used as printing paper for the complainant's invoice.

7. In support of the foregoing, the Organisation provided the Commission with a document entitled, "*Policies and internal guideline* [*sic*] *for the protection of personal data of customers as at November 2016*". The document provided for, amongst other things, (a) all invoices to be printed on new paper (b) the supervisor to check that the invoices are printed on new paper instead of reused paper containing customer's information (c) the delivery man to check the invoices to ensure that the back of the invoices do not contain other customers' information (d) the acknowledgment copy of the invoices be destroyed after delivery man returns the copy to the Organisation (e) the Organisation's customer information to be kept safe. The Organisation claimed that some of the policies set out in the document had already been implemented prior to November 2016.

8. The Organisation admitted that none of its staff had undergone any training in respect of the Organisation's obligations under the Personal Data Protection Act 2012 ("**PDPA**"). Further, no training was conducted to explain the Organisation's own internal policies and guidelines to its staff. However, the Organisation claimed that management had briefed staff on the internal policies and guidelines at an unspecified meeting.

B. COMMISSION'S FINDINGS AND ASSESSMENT

(i) There was an unauthorised disclosure of personal data

9. The information disclosed by the second invoice is personal data within the meaning of section 2 of the PDPA, which requires that the individual may be identified from the data. Given that the surname of the customer was provided, along with the customer's address, e-mail address, and telephone number, it was possible to identify that customer solely from the information disclosed by the second invoice.

10. Given that the disclosure of such information contained in the second invoice was made without consent or authority under the PDPA (or other written laws), it was an unauthorised disclosure of personal data under the PDPA.

(ii) The unauthorised disclosure was the result of a breach of the Organisation's obligation to make reasonable arrangements for the protection of personal data

11. The Organisation claims that the unauthorised disclosure was an isolated incident that occurred due to the negligence of its staff. Specifically, that someone accidentally placed the second invoice in the printing tray instead of destroying it. In this regard, it could be argued that the unauthorised disclosure was simply caused by a one-off mistake by the Organisation's staff, and not due to any lack or failure to put in place "reasonable security arrangements" under section 24 of the PDPA.

12. From the Commission's investigations, though, there were more deep-rooted problems with the Organisation's processes, and it lacked the necessary policies and practices to protect personal data. These failures and omissions by the Organisation are detailed below.

(a) The Organisation effectively did not have any policy in place to protect personal data

13. The Organisation had produced to the Commission a copy of its data protection policy which it says was put in place in November 2016. This is the same month in which the data breach had taken place. Prior to this, the Organisation claims it did not have a written policy on the protection of personal data.

14. The 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.

15. In relation to the Organisation's data protection policy itself, it consisted of a mere six bullet points. At least three of the six points in the policy relates coincidentally to the data breach incident – for example, it provides that the supervisor has to check that the invoices are printed on new paper instead of reused paper containing customer's information. Additionally, the policy was put in place the same period of time as the data breach incident. The combination of the timing and content of the policy raises suspicion, and the Commission cannot rule out the possibility, that it was created subsequent to the breach to address that particular incident.

16. Additionally, investigations did not reveal any evidence to show that steps were taken to implement the data protection policy that the Organisation had put in place. Some of the evidence that ought ordinarily

to have presented would be internal communications of the data protection policy to staff, internal briefings conducted to raise staff awareness and training events and collateral to educate staff. During the investigation, the Commission specifically asked the Organisation what other arrangements, apart from the policy documents that they had already produced, the Organisation had in place to mitigate the risk of an unauthorised disclosure of personal data on the printed invoices. The Commission also asked for documentary evidence of such arrangements. The Organisation replied that it had assigned "a supervisor" to ensure that signed invoices were destroyed at the end of each business day, and even suggested that the supervisor was there to check that "*invoices were not printed on the reverse side of invoice paper*". However, there were several issues which cast doubt on the Organisation's response:

a. The Organisation did not produce any documentary or other proof of its processes and workflow to show the supervisor's place and role in the relevant process or workflow;
b. Likewise, there was no indication of the actions or tasks that the supervisor was supposed to perform as part of the supervisory checks in the overall invoice process; and
c. There was no explanation why the supervisor did not pick up on the erroneous invoices (when that was the precise risk that the supervisor was tasked to spot).

In the premises, the Commission assessed the Organisation's claim that it had an effective supervisory check put in place as no more than a bare assertion that was not adequately supported by facts disclosed during investigations. In the final analysis, the Commission is not satisfied by the Organisation's response that the Organisation had translated its policies (if any) to effective practices to protect personal data.

17. From the above, given the shortcomings in the Organisation's data protection policy, and the absence of evidence in its implementation, the Commission is not satisfied that the Organisation had an *effective* data protection policy at the time of the data breach incident to protect personal data.

18. Next, the Organisation admitted that it did not provide any data protection training whatsoever to its employees. Again, staff training forms part of the effective measures to protect personal data. The Commission has emphasised the importance of training in its Advisory Guidelines[1], and also in its decision *In the Matter of National University of Singapore*[2]*.* The Commission agrees with the view expressed by the Office of the Australian Information Commissioner:

---

[1] PDPC, *Advisory Guidelines on Key Concepts in the PDPA* (revised 15 July 2016) <https://www.pdpc.gov.sg/legislation-and-guidelines/advisory-guidelines/main-advisory-guidelines#AG1> at [17.5].
[2] [2017] SGPDPC 5 at [21] to [28].

"*Regular staff training, and a culture of privacy awareness are essential to ensure compliance.*"[3]

19. Overall, it is clear that the Organisation did not make reasonable security arrangements for the protection of personal data:

    a. The Organisation's data protection policy was formalised during the month that the data breach occurred and could have been formalised after the unauthorised disclosure took place;

    b. There was no evidence to show that steps had actually been taken to implement such policy prior to the breach; and

    c. Further, the Organisation admitted that its staff had no training whatsoever regarding their data protection obligations.

(b) At a more basic level, the Organisation did not seem to engage in the issue of what it should do to protect personal data. It had simply relied on its employees carrying out their jobs correctly.

20. A further point must be made. Based on the Organisation's representations, it would appear that the Organisation is essentially relying on its employees and staff carrying out their job functions correctly to say that this is a form of data protection measure in and of itself. If the employees and staff had printed and sent the correct invoice to the correct recipient, there would not be any data protection issue to begin with.

21. In the Commission's view, it is not enough for the Organisation to simply rely on its staff and employees to carry out their duties correctly for the protection of personal data. An organisation has certain obligations with respect to personal data that it has collected and which is holds or has control over. One such obligation is to put in place policies and measures to protect the personal data and to prevent unauthorised use, disclosure or alteration. Policies pertinent and adapted to the Organisation's business and processes ought to be crafted and disseminated to staff. Indeed, section 12(c) of the PDPA imposes an obligation for such policies and practices to be communicated to staff. An effective mode of communication is to provide training to staff, whether in traditional classroom settings or through other means such as online training.

22. Crucially, it is important for the management of a company to "buy-in" to adopting good data protection practices for the company. It is from this starting point – the management level – that the company's policies and

---

[3] *Office of the Australian Information Commissioner, Introduction to the APPs and OAIC's Regulatory Approach (May 2005) <https://www.oaic.gov.au/agencies-and-organisations/training-resources/introduction-to-the-apps-and-the-oaic-s-regulatory-approach> at p 24.*

practices be formulated with data protection in mind. From there, such good data protection policies and practices can permeate down to and be adopted at the staff level of the company. The Commission agrees with the observation made by the Australian Information Commissioner and Privacy Commissioner of Canada in the joint investigation into *Ashley Madison*:

> *"Having documented security policies and procedures is a basic organizational security safeguard, particularly for an organization holding significant amounts of personal information. Making informational policies and practices explicit provides clarity about expectations to facilitate consistency, and helps to avoid gaps in security coverage. It also sends key signals to employees about the importance placed on information security. Furthermore, such security policies and processes need to be updated and reviewed based on the evolving threat landscape, which would be very challenging if they are not formalized in some manner."*[4]

23. The above position also stresses the importance of having documented policies, as mentioned at paragraph 14 above.

24. It is also important that management actively supervises employees and takes responsibility for creating a culture of security-awareness. As observed by the Hong Kong Privacy Commissioner for Personal Data:

> "*With sound security policies and procedures in place, there is no guarantee that they will be followed. In this regard, supervision and monitoring of the implementation of the procedures are important."*[5]

25. Similarly, in its investigation into *Monarch Beauty Supply*, the Office of the Alberta Privacy Commissioner found that the Store Manager and District Manager of the organisation had not been diligent, as they had simply assumed that employees would shred documents containing customers' credit and debit card information, in line with the organisation's policies. However, as management had not provided sufficient instruction on the care and disposal of sensitive documents, the employees in fact threw the documents into the dumpster, which resulted in customers' personal data falling into the hands of criminal suspects[6]. *Monarch Beauty Supply* is an example of what could go wrong and the harm that results from disclosure of personal data due to

---

[4] *PIPEDA Report of Findings #2016-005: Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/> at* [65].

[5] *Investigation Report: Hong Kong Police Force's Repeated Loss of Documents Containing Personal Data (R13 – 0407) <https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R13_0407_e.pdf> at* [38].

[6] *Order P2006-IR-003: Monarch Beauty Supply [a division of Beauty Systems Group (Canada) Inc.]* <https://www.oipc.ab.ca/media/127842/P2006-003IR.pdf> at [40(2)].

insufficient follow through on the part of management. The Commission therefore highlights that management has an obligation to establish the standard of care that it expects staff to observe, communicate and train staff, and to put in place appropriate supervision and monitoring to ensure compliance.

26. In this case, for the reasons mentioned above, the Organisation did not have in place, whether at the management or staff level, the necessary policies to protect personal data. It has therefore failed in its obligation to protect personal data under section 24 of the PDPA.

C. ENFORCEMENT ACTION BY THE COMMISSION

27. Given that the Organisation breached its obligation under section 24 of the PDPA, the Commission is empowered under section 29(1) of the PDPA to issue such directions as it thinks fit in the circumstances.

28. The Commission has decided to issue the following directions to the Organisation:

    a. To review its policy for the protection of personal data in relation to its order fulfilment process;

    b. To develop procedures to ensure effective implementation of its data protection policy; and

    c. To conduct training to ensure that its staff are aware of, and will comply with, the requirements of the PDPA when handling personal data.

29. The following mitigating factors were taken in account in arriving at this decision:

    a. The unauthorised disclosure was made to a single person only;

    b. The personal data disclosed was not sensitive; and

    c. There was no evidence that any loss or damage was caused by the unauthorised disclosure.

YEONG ZEE KIN
DEPUTY COMMISSIONER
PERSONAL DATA PROTECTION COMMISSION