PERSONAL DATA PROTECTION COMMISSION

[2017] SGPDPC 18

Case No DP-1610-B0261

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

And

Credit Counselling Singapore

… *Organisation*

GROUNDS OF DECISION

Credit Counselling Singapore

[2017] SGPDPC 18

Tan Kiat How, Commissioner — Case No DP-1610-B0261

29 December 2017

Background

1 An admin staff of Credit Counselling Singapore ("**CCS**" or "the **Organisation**") had sent out a mass email to 96 individuals of the Organisation's debt management programme ("**DMP**"), which exposed their email addresses and associated names (for some individuals) to all recipients. The Commissioner found this to be an unauthorised disclosure of personal data, including the identity of individuals' who were on the DMP. The Commissioner found the Organisation to be in breach of its Protection Obligation under the Personal Data Protection Act 2012 ("**PDPA**"). The Commissioner's findings and grounds for his decision are set out below.

Material Facts

2 The Organisation is a registered charity under the National Council of Social Services. The Organisation provides assistance to debt-distressed individuals (whom it calls "**clients**"), such as credit counselling and facilitating the establishment of a debt restructuring plan with creditors. The DMP is a voluntary debt repayment scheme under which the Organisation helps clients, who are facing difficulties or unable to repay their unsecured consumer debts, to work out a payment arrangement with their creditors.

3 The data breach occurred when the Organisation sought to obtain a status update from its clients on the debts to be repaid to their creditors under the DMP. At the material time, the Organisation had a total of [redacted] 'active' DMP clients, of which 810 clients had received the questionnaire from the Organisation via post requesting for a repayment status update. Of these 810 clients, 297 clients failed to respond by the deadline. The Organisation then sent three batches of follow-up emails to these 297 DMP clients.

4 On 30 September 2016, an admin staff of the Organisation made a mistake when sending out one of the three batches of follow-up emails (the "**Follow-up Email**"). Instead of pasting the email addresses of 96 DMP clients in the "Bcc" field, the admin staff had inadvertently pasted the email addresses in the "To" field before proceeding to send the Follow-up Email out. This mistake caused the 96 email addresses and associated names (for some individuals) to be displayed in the "To" field and were thus visible to all the recipients of the Follow-up Email.

5 Subsequently, the Organisation received feedback from four DMP clients who were concerned that their identity had been disclosed to the rest of the recipients. In addition, two DMP clients had clicked the "Reply All" button when submitting their completed questionnaire to the Organisation, which resulted in inadvertent disclosure of additional personal data (contained in the questionnaire) to all the other recipients.

The Commissioner's Findings and Basis for Determination

Main Issues for Determination

6 The issues to be determined in the present case are as follows:

(a) whether the information disclosed by the Follow-up Email constituted personal data; and

(b) whether the Organisation had put in place reasonable security arrangements to protect the personal data set in its possession or in its control, as required under section 24 of the PDPA.

Issue (a): Whether the information disclosed by the Follow-up Email constituted personal data

7 The starting point is whether the Follow-up Email that was sent out by the Organisation had disclosed personal data of the 96 DMP clients.

(i) The 96 email addresses were personal data

8 Section 2(1) of the PDPA defines "personal data" to be data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access. In this case, all 96 email addresses disclosed in the Follow-up Email are considered personal data under the PDPA because the Organisation would also have the name of individual to whom the email address belongs to, and would thus be able to identify the individual from that email address. The Protection Obligation therefore attaches to the email addresses both as part of the Organisation's complete records of its DMP clients as well as when used on their own.

9 A copy of the Follow-up Email that was provided to the Personal Data Protection Commission ("**PDPC**") revealed that there were three categories of email addresses: (a) an email address which disclosed the full name of the individual, eg "tan.ah.kow980@gmail.com"; (b) an email address which contained the partial name of the individual, eg "ylt.rachel@hotmail.com"; and

(c) an email address from which no individual's name could be deciphered eg "foodlover721@hotmail.com".[1] Prima facie, the disclosure of email addresses coming under categories (a) and (b) would allow an outsider to identify the individual because the name or partial name of the individuals have been disclosed. Therefore, even from the perspective of an outsider, the Follow-up Email had disclosed personal data of individuals to the outsider for categories (a) and (b) above.

10 Additionally, investigations revealed that out of the 96 email addresses that were disclosed, 16 individuals could be identified on online social media platforms based on a search of their email addresses. As stated above, the definition of "personal data" under the PDPA includes data that can be identified from (a) that data coupled with (b) other information to which the organisation has or is likely to have access. Since the "other information" that is needed to identify the 16 individuals behind the email addresses disclosed is readily available on various social media platforms, the email addresses of those 16 individuals would allow a person who had access to the email addresses to identify the 16 individuals. In this day and age where access to the Internet is prevalent and there is widespread use of social media platforms, it would be unrealistic to ignore the Internet as a source of information to identify an individual.

---

1 For the avoidance of doubt, these examples are not the actual email addresses disclosed in the data breach and are purely for illustration purposes only. Any resemblance to an actual email address is purely coincidental, and there is no intention to identify any individual.

(ii) The context of the Follow-up Email rendered the communication content and personal data sensitive

11 This is a case where the personal data, in the form of contact details, which ordinarily would not have been sensitive were rendered sensitive by reason of the context of their disclosure. The nature and context of the Follow-up Email is crucial to this analysis. As mentioned above, the Organisation had sent the Follow-up Email as part of the periodic update from its DMP clients to obtain the status of their debt repayment. The Follow-up Email contained a "DMP Status Update Form" in which individuals were required to provide the Organisation with information about their state of indebtedness by selecting one of several available options. For example, one option was "*I have completed my DMP repayment to all my creditors…Please assist to remove my DMP status from my Credit Bureau Singapore's credit report*". Another available option was "*I am servicing my DMP repayment every month with no missed payment in the last 12 months*." Yet another option that individuals could select was "*I have missed one or more payments in the last 12 months and I wish to seek assistance from CCS. I will contact CCS within the next two weeks to discuss my case*." Further down the form, the individual was to fill up his particulars, including his name and NRIC number.

12 Given the above, the fact that an individual is included on the list of email addresses in the Follow-up Email would indicate that the individual is either currently facing financial debt, or was previously in debt, and that the individual is obtaining, or had previously obtained, assistance under the DMP scheme to pay off the debt.

13 Therefore, if an individual's identity had been revealed by the disclosure of his or her email address in the Follow-up Email, it would also mean that the

individual's financial information (i.e. his debt status as a current or former debt-distressed individual) would be divulged by the Follow-up Email.

14 At the time when the Follow-Up Email was sent out by the Organisation, it contained a blank DMP Status Update Form, and hence, no other personal information of individuals was disclosed to the recipients of the Follow-Up Email beyond the disclosure of the individual's financial information.

15 That the financial information is sensitive personal data of an individual is a position that has been taken by the Commissioner, as well as foreign data protection authorities.

16 In the earlier decisions of the PDPC, the PDPC found that financial information such as a policyholder's bank account details (consisting of the name of the bank, branch of the bank, the bank account number and the account holder's name);[2] and an individual's central depository account details (consisting of the account holder's name, address, account number, securities holdings, transaction and payment summaries)[3] to be personal data that is of a sensitive nature.

17 The Information & Privacy Commissioner for British Columbia has taken a similar position in a case involving the unauthorised disclosure of the names of the members of the trade unions, as well as the amount of strike pay they were paid and still owed to the union, the commissioner took the view that:[4]

---

2 *Re AIA Singapore Private Limited* [2016] SGPDPC 10 at [5] and [19].

3 *Re Central Depository (Pte) Limited and another* [2016] SGPDPC 11 at [8] and [24].

4 *Order P17-01: Construction Maintenance and Allied Workers Local 2423* <https://www.oipc.bc.ca/orders/2020> at [39].

> "financial information connected to an individual is generally sensitive information, particularly when it involves a debt. Owing money to another party (whether an individual or any legal entity) is generally a private matter between those parties. In my view, the fact that money was borrowed and is owed could, whether justified or not, lead to moral judgements about the individuals and their spending, financial choices, earning power or about their character generally. In particular, a lapse in, or lack of, payment to that party may be considered particularly sensitive information, given the stigma that may be attached to an individual having a delinquent debt."
>
> [Emphasis added.]

18 In another Canadian case, the Information and Privacy Commissioner of Alberta found that the actions of an employee of an organisation, who had disclosed personal data (comprising an individual's name, telephone number, creditor name, amount owing, last payment amount, last payment date and unique account number) to an unauthorised third party debt settlement agency, had caused there to be a real risk of significant harm posed to the affected individuals. In finding the organisation in breach of the Personal Information Protection Act (PIPA), the commissioner stated that:[5]

> "the personal information involved could be used to cause harm to affected individuals in the form of financial loss, embarrassment and harassment by an unauthorized third party debt collection agency. In my view, these are significant harms."
>
> [Emphasis added.]

Given the type of sensitive personal data disclosed, the Commissioner took the position that this would give an unauthorised debt collection agency "*enough personal information to potentially convince affected individuals it is*

---

5 *P2015-ND-02: CBV Collection Services Ltd.* <https://www.oipc.ab.ca/media/386982/P2015_ND_02.pdf> at p. 3.

authorized to collect the debt",[6] which would then lead to the abovementioned harms.

19 Disclosure of an individual's indebtedness to other third parties could lead to harm to the individual because it could result in social stigma, discrimination or tarnish his reputation. These are real possibilities that can affect a person's life. Hence, the confidentiality of the individual's financial information should not be treated lightly.

20 The above view is captured in the comments provided by the Information Commissioner's Office ("**ICO**") in its Guide to data protection. When considering the definition of 'sensitive personal data' under the UK Data Protection Act 1998, the ICO explained that "*[the] presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data*."[7]

21 It is also worth pointing out that the Office of the Privacy Commissioner of Canada ("**OPC**") has taken the position that "*a simple reference to an outstanding debt, even without disclosing specific details about the debt, is personal information*".[8] In that case, a bank had telephoned the complainant's

---

6 *P2015-ND-02: CBV Collection Services Ltd.* <https://www.oipc.ab.ca/media/386982/P2015_ND_02.pdf> at p. 3.

7 UK, ICO's Guide to data protection: Key definitions of the Data Protection Act (7 July 2017) <https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/> at p. 4.

8 See OPC, Interpretation Bulletin: Personal Information (October 2013), Part III: Application in Different Contexts <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-

employer after a confrontation between the complainant and a bank manager. The employer's internal affairs bureau then sent an internal email which stated that the complainant was involved in a civil dispute with the bank, and that he had "*incurred a sizeable debt and was under financial pressure*".[9] The commissioner found that this internal email containing that single reference to the complainant's indebtedness and financial situation was personal information that should not have been disclosed.

22 In Hong Kong, the Officer of the Privacy Commissioner for Personal Data ("**PCPD**") has taken the position that financial information, including an individual's indebtedness, constitutes sensitive data. The PCPD's Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry provides that:[10]

> "[information] showing the financial problems of a customer such as default in payment is commonly recognised as sensitive data, and should therefore be handled with extra care. Such data should not be disclosed to any third party unless there is a real need to do so."
>
> [Emphasis added.]

---

bulletins/interpretations_02/#fn41> at fourth bullet point in the "Financial Context" section, p. 3.

9 *PIPEDA Case Summary #2003-267: Bank discloses customer's personal information to employer* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2004/pipeda-2004-267/> at p. 1.

10 HK, PCPD, Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry (October 2014) <https://www.pcpd.org.hk/english/resources_centre/industry_specific/files/GN_banking_e.pdf> at [3.82].

The Guidance goes on to suggest measures that organisations can take when sending mail to debtors in order to avoid situations where the debtor's personal data is divulged to or accessed by unintended recipients.

23 Accordingly, the personal data that was disclosed in this case was not ordinary personal data but "sensitive" personal data. As will be elaborated on below, when it comes to the protection of "sensitive" personal data, organisations are required to take extra precautions and ensure higher standards of protection under the PDPA.

24 Given that the disclosure of email addresses was made by the Organisation inadvertently (as opposed to an *intentional* one), the issue for determination is whether the Organisation had put in place reasonable security arrangements to protect the personal data of its DMP clients against unauthorised disclosures pursuant to section 24 of the PDPA.

Issue (b): Whether the Organisation has complied with its Protection Obligation under Section 24 of the PDPA

(i) Stronger controls and greater measures needed to protect sensitive personal data

25 When it comes to the protection of sensitive personal data, there is a need to put in place stronger security measures because of the actual or potential harm, and the severity of such harm, that may befall an individual from a misuse or unauthorised use of such data. The Advisory Guidelines on Key Concepts in the PDPA state that an organisation should "*design and organise its arrangements to fit … the possible harm that might result from a security breach*", and to "*implement robust policies and procedures for ensuring*

appropriate levels of security for personal data of varying levels of sensitivity".[11]

26 Some examples of these precautions to protect sensitive personal data include, but are not limited to, good email procedures and encryption technology. The Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data specifically encourages organisations to undertake security measures to prevent the sending of personal data to the wrong recipients, including "*[implementing] email procedures to ensure all emails sent externally to a group of recipients have the recipients' email addresses placed in 'bcc' fields to avoid disclosing recipients' email addresses to all other recipients of the email*".[12] In another example, the Guide to Securing Personal Data in Electronic Medium suggests organisations adopt encryption as a security measure when emails contain confidential or sensitive personal data that "*has a higher risk of adversely affecting an individual if such personal data is compromised*."[13]

27 In adopting this view on implementing greater safeguards for more sensitive personal data, the Commissioner agrees with the observations made by the OPC in the *PIPEDA Report of Findings #2014-003* that organisations "*must protect personal information by implementing security safeguards appropriate to the sensitivity of the information*" and that the "*more sensitive*

---

11 PDPC, Advisory Guidelines on Key Concepts in the PDPA (revised 27 July 2016) at [17.3].

12 PDPC, Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data at [2.1], ninth bullet point, p. 5.

13 PDPC, Guide to Securing Personal Data in Electronic Medium (revised 20 January 2017) at [14.3].

information should be safeguarded by a higher level of protection".[14] In that case, the OPC found that an insurance company had lost its policyholders' files containing sensitive personal data as the safeguards for the control and tracking of the insurance files at the time of the data breach incident were inadequate.

(ii) The Organisation failed to implement adequate administrative security measures

28 The Organisation's mistake of pasting the list of recipient email addresses in the "To" field instead of the "Bcc" field was a straightforward one, and could have been quite easily repeated. All it takes is just a few "wrong" clicks of the button, and the list of email addresses could be pasted in the wrong field and sent out with the unauthorised disclosure of email addresses. Yet the impact of the unauthorised disclosure cannot be ignored – personal information of 96 clients, including their sensitive financial information, have been disclosed with the potential that such disclosure may cause harm to these individuals.

29 It is precisely that the mistake can be so easily *made* and *repeated* which draws into focus the issue with the Organisation's arrangements to protect personal data. The Organisation did not have the appropriate checks and controls to prevent or minimise such mistakes from occurring (which could easily happen again). The types of checks and controls to be implemented could range from an additional layer of supervision or oversight before the email is sent, to sending such emails individually (eg using the mail merge function of

14 *PIPEDA Report of Findings #2014-003: Insurance company overhauls its security safeguards following privacy breach* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2014/pipeda-2014-003/>, first and second bullet points in the "Lessons Learned" section at p. 2.

Outlook). Whatever the way, the staff runs through the important steps to be taken with his or her supervisor, who can provide guidance or corrections to the staff before the action is carried out. Alternatively, it could be in the form of a technical control which ensures that the email addresses are correctly pasted in the "bcc" field of the email instead of the "To" field. The Organisation, however, did not have any checks or controls in place.

30 The Commissioner is not suggesting that organisations would need, for example, to have the added layer of supervision in *all* cases where emails containing personal data are being sent out. As mentioned above, organisations are to put in place security arrangements that are commensurate with the sensitivity of the data in question – a balance of considerations. In relation to personal data that is of a **non-sensitive** nature, it may be the case that a second layer of checks is not needed for admin staff to send out the email, if, for example, the admin staff has gone through the relevant training on data protection.

31 However, since the personal data here was of a sensitive nature, the Organisation needed to implement a higher level of security to protect the data (as so described at paragraphs 25 to 27 above). As mentioned above, the Organisation's lack of any checks and controls was unacceptable in the given context. Moreover, the Organisation did not seem to have taken any steps towards protecting the personal data. This is evident from the lack of differentiation, in the Organisation's processes, between an email that was sent out by the Organisation which *did not* contain personal data, and an email which contained personal data (and sensitive personal data). In both cases, the admin staff was able to send out the email indiscriminately, without requiring further precautions or steps to be taken to protect those emails which contained personal data.

32 The nature of the Organisation's work is a relevant factor to be taken into consideration. It routinely handles large volumes of sensitive financial personal data of individuals. This being the case, it is foreseeable that there will be risks of inadvertent disclosure of sensitive personal data. The process in which emails containing reminders to submit repayment status updates are sent to its clients ought to have been identified as one which carries with it a significant risk of inadvertent disclosure. There was therefore no excuse for the Organisation not to already have a system of checks and controls in place to prevent or minimise such unauthorised disclosure of personal data. As a matter of good practice, the Organisation could have also carried out a data protection risk assessment, which would have helped to identify and address the specific risk of disclosure that has arisen in this case.

33 The Organisation mentioned that, at that time, it had planned to put in place a "mail-merge" software which would allow for mass emails to be sent individually to clients. But it had only started using it from November 2016 onwards; by which time the Follow-up Email had already been sent out (it was sent out on 30 September 2016). The fact that there was a solution like the "mail-merge" software which could have ameliorated the risks of unauthorised disclosure of personal data also exemplifies the Commissioner's position that the Organisation could have done more to protect the personal data of their clients. With the benefit of hindsight, perhaps this incident would have been avoided had the mail merge solution been implemented sooner.

34 Given the Commissioner's findings above that the Organisation has not put in place adequate security arrangements to protect the personal data of its clients, it is therefore concluded that the Organisation was in breach of the Protection Obligation under section 24 of the PDPA.

The Commissioner's Directions

35 In respect of the Commissioner's findings that the Organisation is in breach of section 24 of the PDPA, the Commissioner is empowered under section 29 of the PDPA to give the Organisation such directions as it deems fit to ensure the Organisation's compliance with the PDPA. This may include directing the Organisation to pay a financial penalty of such amount not exceeding S$1 million as the Commissioner thinks fit.

36 In assessing the breach and determining the directions to be imposed to the Organisation in this case, the Commissioner took into account the following aggravating factors:

(a) information about an individual's adverse financial condition and/or state of indebtedness was sensitive personal data, and the disclosure of which could cause actual or potential harm, injury or hardship to the individual, including serious reputational damage and embarrassment;

(b) given the nature of the Organisation's business of handling large volumes of sensitive personal data, the Organisation ought to have put in place a system of checks for any sensitive personal data that may be disclosed, but it did not do so; and

(c) the data breach incident may cause members of the public to lose trust in such credit counselling organisations to safeguard their personal data, which may frustrate the larger national credit management efforts.

37 The Commissioner also took into account the following mitigating factors:

(a) the Organisation had cooperated fully with the Commissioner's investigations and had readily admitted its mistake without delay;

(b) the Organisation had promptly notified all the affected recipients of the data breach incident and offered them an apology alongside a request to delete the Follow-up Email;

(c) the Organisation has counselled the admin staff who made the mistake, and has taken further steps to prevent future data breaches such as its plans to conduct an organisation-wide refresher course on compliance with the PDPA, and deploying the "mail-merge" software, mentioned above, within two months; and

(d) there were no other data breach incidents reported apart from this one.

38 Having carefully considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to pay a financial penalty of S$10,000 within 30 days from the date of the Commissioner's direction, failing which, interest, at the rate specified in the Rules of Court in respect of judgment debts, shall be payable on the outstanding amount of such financial penalty.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION