# Habitat for Humanity Singapore Ltd

**[2018] SGPDPC 9**

Yeong Zee Kin, Deputy Commissioner — Case No DP-1707-B0971

**Data Protection** – Openness obligation – Requirement to develop and implement policies and practices and communicate these policies and practices to staff

**Data Protection** – Protection obligation – Disclosure of personal data – Insufficient administrative security arrangements

**Data Protection** – Personal data – Unnecessary disclosure of NRIC numbers – Stronger controls needed to protect sensitive personal data

3 May 2018

## Background

1 On 20 July 2017, the Organisation sent out an email to 32 of its volunteers with a PDF attachment comprising a batch of community involvement programme ("**CIP**") letters (the "**CIP Letters**") acknowledging the participation of each volunteer at an event organised by the Organisation (the "**Incident**"). The Personal Data Protection Commission (the "**PDPC**") was informed of the Incident on 22 July 2017 and commenced its investigations thereafter. I set out below my findings and grounds of decision based on the investigations carried out in this matter.

**Material Facts**

2 The Organisation is a registered charity under the National Council of Social Services, which objectives include seeking to eliminate poverty housing worldwide by providing decent and affordable housing. In furtherance of its objectives, the Organisation organises community involvement programmes, where volunteers can participate in activities such as mass clean-up events. After such events, the Organisation would generally send out a CIP letter to acknowledge and verify each individual volunteer's participation.

3 The Incident involved the disclosure of a batch of CIP Letters in an email (the "**Email**") that was prepared by a manager (the "**Manager**") in the Organisation. The CIP Letters were created using the mail merge function in Microsoft Word which would fill in a CIP letter template with the names and NRIC numbers of the volunteers. This created a single Microsoft Word document containing the CIP Letters for all the volunteers, which the Manager then converted from Microsoft Word to PDF format. The Manager then sent the PDF containing the entire batch of CIP Letters to another member of staff ("**Admin Staff**"), along with the volunteers' email addresses and instructed the Admin Staff to send out the CIP Letters.

4 The Organisation's usual practice was for the document containing the entire batch of CIP Letters to be segregated and split into individual CIP Letters before each CIP Letter was individually sent to its respective volunteers. However, in this case, neither the Manager nor the Admin Staff had prepared and/or handled any CIP Letters prior to the Incident. The Manager failed to instruct the Admin Staff on the proper procedure.

5 On 20 July 2017, the Admin Staff sent a mass email to all the volunteers who were involved in the mass clean-up event, attaching the PDF document

which contained the entire batch of CIP Letters. As a result, the PDF attachment containing the CIP Letters revealed the names and NRIC numbers of all the volunteers who had participated in the Organisation's mass clean-up event. Additionally, the Email was also sent with the email addresses of all the recipients in the "cc" field. Consequently, the Organisation received two emails from the volunteers who had received the Email, expressing their concern that their personal data had been disclosed to other parties without their consent.

**Findings and Basis for Determination**

6 The issues for determination are:

(a) whether the Organisation complied with its obligations under section 12 of the PDPA; and

(b) whether the Organisation was in breach of section 24 of the PDPA.

7 As a preliminary point, the names, NRIC numbers and email addresses disclosed in the Email and CIP Letters fall within the definition of "personal data" under section 2(1) of the PDPA, as it was clearly possible to identify an individual from that data.

8 Pursuant to section 53(1) of the PDPA, any act done or conduct engaged in by a person in the course of his employment shall be treated for the purposes of the PDPA as done or engaged in by his employer as well as by him, regardless of whether it was done or engaged in with the employer's knowledge or approval. The Organisation is therefore responsible for its employees' conduct in relation to the Incident.

***(a) Whether the Organisation complied with its obligations under section 12 of the PDPA***

9 Section 12(a) of the PDPA requires an organisation to develop and implement policies and practices that are necessary to meet its obligations under the PDPA. Section 12(c) of the PDPA also requires the organisation to communicate to its staff information about such policies and practices.

10 The Organisation claimed to have instructed its employees on the Organisation's obligations under the PDPA and the importance of safeguarding its volunteers and donors' personal data. Employees who were required to deal with personal data were also briefed on the following data protection practices and procedures "on a need basis":

(a) to use the "bcc" function when sending out mass emails;

(b) to send the CIP Letters individually;

(c) to avoid sharing collected personal data with unauthorised third parties;

(d) to contact individuals only for purposes that they have given consent;

(e) to use personal data only for the purposes for which it was collected; and

(f) to secure all documents containing personal data safely.

11 However, there were no documented policies, practices or procedures in relation to sending out the CIP Letters. Indeed, the Incident could very well have been averted if the Organisation had implemented, and documented, a standard

operating procedure for the sending out of the CIP Letters. By the Organisation's own admission, the Manager had omitted to instruct the Admin Staff on the Organisation's usual procedure for sending out the CIP Letters and she "*should have written down the instruction clearly for [the Admin Staff], which [she] had forgotten to do*."

12 I take this opportunity to reiterate the benefits and importance of documenting an organisation's data protection policies and practices in a written policy as emphasised in *Re Furnituremart.sg* [2017] SGPDPC 7 ("***Furnituremart.sg***") at [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."

13 In this regard, the Organisation was unable to demonstrate or produce any evidence that it had developed and implemented policies and practices necessary for it to comply with its obligations under the PDPA in respect of sending out the CIP Letters.

14 In addition, the Organisation did not provide any formalised data protection training for its employees. As the Commissioner observed in *Re National University of Singapore* [2017] SGPDPC 5 (at [21]), data protection training may fall under both the openness obligation (specifically, section 12 of the PDPA) and the protection obligation (section 24 of the PDPA). Data protection training is an effective mode of communication of the Organisation's

policies and practices to fulfil the openness obligation (section 12(c) of the PDPA).

15 The Manager's failure to communicate the Organisation's data protection policy was evidenced by the Admin Staff's lack of awareness of the use of the "bcc" function and the implications of her actions in respect of the Email. Although the Admin Staff claimed to have been instructed on the "*rules with regard to volunteers' personal details*", the fact that she: (a) did not query whether it was appropriate to send the entire batch of CIP Letters containing personal data to all the volunteers; and (b) did not think to check whether the email addresses of the recipients of a mass email should be inserted in the "bcc" field instead of the "to" or "cc" fields suggests that there was a lack of awareness of the Organisation's obligations under the PDPA.

16 Accordingly, I find that the Organisation has breached its openness obligation, given that it did not develop and implement a data protection policy as necessary for the Organisation to meet its obligations under the PDPA at the time of the Incident, and it did not communicate its data protection policies and practices to its staff, as required under sections 12(a) and (c) of the PDPA.

### *(b) Whether the Organisation was in breach of section 24 of the PDPA*

17 Section 24 of the PDPA requires an organisation to protect the 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.

18 In this case, the Organisation's informal practices and verbal reminders "on a need basis" were an insufficient security arrangement for the purposes of compliance with section 24 of the PDPA. The Organisation did not implement

any checks and controls to prevent or minimise the risk of unauthorised disclosure of personal data. Knowing that the output produced by the Microsoft Word mail merge function was a single file containing the CIP Letters for all volunteers in the batch, the Organisation did not implement technical arrangements such as installing IT tools[1] that would have enabled the CIP Letters to be generated from the CIP letter template as separate documents. At the minimum, greater awareness of the need to protect the personal data of volunteers would have prompted the Admin Staff to process the PDF or Microsoft Word document containing the entire batch of CIP Letter manually in order to split the document into individual PDF files. The Manager would also have had a role to play in ensuring that this was done and could have implemented simple process checks to identify errors. Furthermore, technical controls could also have been installed to remind employees to use the "bcc" function when multiple email addresses are pasted in the "to" or "cc" field.

*Unnecessary disclosure of NRIC numbers*

19 At this juncture, I observe that the disclosure of the volunteers' NRIC numbers in the CIP Letters was unnecessary as the CIP Letters had already referred to the volunteers by their full names. Given that an individual's NRIC number is a permanent and irreplaceable identifier which can be used to unlock large amounts of information relating to the individual, organisations should not disclose an individual's NRIC number except where it is required under the law or where it is necessary to accurately establish and verify the identity of the individual by way of the same. It is not apparent to me that the need to identify

1 There were IT tools reasonably available that would have enabled the CIP Letters to be generated from a template as separate documents. For instance, the installable PDF Split & Merge program allows a single PDF or Microsoft Word output from a mail merge operation to be processed into individual PDF files.

an individual in a CIP Letter was to such a degree of specificity that his or her NRIC had to be included. The nature and function of a CIP Letter did not necessitate the publication of the volunteer's NRIC number.

20 Organisations that choose to disclose more sensitive data than are required for their business or legal purposes have to be able to defend such decisions and bear the burden of ensuring an appropriate level of security for the personal data of varying levels of sensitivity. As observed in *Re Aviva Ltd* [2017] SGPDPC 14 (at [18]):

> "The Advisory Guidelines on Key Concepts in the PDPA states that an organisation should "implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity". **This means that a higher standard of protection is required for more sensitive personal data**."
>
> [Emphasis added.]

21 In the premises, I find that the Organisation failed to make reasonable security arrangements to protect the personal data in its possession and control, as the Organisation:

(a) did not put in place basic administrative security arrangements such as setting out its data protection policies and procedures in writing;

(b) did not implement any checks and controls to ensure that its employees were complying with its data protection practices and policies;

(c) did not provide any formalised data protection training for its employees;

(d) failed to properly supervise the employees who were in charge of preparing and sending out the CIP Letters; and

(e) did not have any other form of security arrangement to protect its volunteers' personal data.

**Directions**

22 Having found that the Organisation is in breach of sections 12(a), 12(c), and 24 of the PDPA, I am empowered under section 29 of the PDPA to give the Organisation such directions as I deem fit to ensure compliance with the PDPA.

23 In assessing the breach and determining the directions to be imposed, I took into account, as an aggravating factor, the fact that the personal data disclosed included the volunteers' NRIC number, which was of a sensitive nature.

24 I also took into account the following mitigating factors:

(a) the disclosure only affected a limited number of people; and

(b) the Organisation had cooperated fully in the PDPC's investigation.

25 Pertinently, the PDPC has recently issued a public consultation on the proposed advisory guidelines for NRIC numbers, which, *inter alia*, discourages the indiscriminate use of NRIC numbers. Due weight has been given to the unsatisfactory practices that currently abound. Our practices as a society need to be improved as we become more knowledgeable about the risks of identity theft and other identity-related risks (and I do not restrict this caution as referring only to online risks). In future, similar conduct may call for the imposition of a financial penalty as proposed changes to the advisory guidelines on the collection, use and disclosure of NRIC numbers are implemented. This case should serve as a clarion call for all organisations to start handling personal

data such as NRIC numbers, which are unique and permanent identifiers of individuals, with a much higher degree of care and discernment than the present.

26 I hereby issue the following directions to the Organisation:

(a) to conduct a review of all its activities involving the handling of personal data of its volunteers and donors;

(b) to put in place a data protection policy, including process safeguards and written internal policies, such as standard operating procedures, to comply with the provisions of the PDPA;

(c) to arrange for personal data protection training for its staff; and

(d) to complete the above directions within 90 days from the date of this decision and inform the Deputy Commissioner of the completion thereof within 1 week of implementation.

**YEONG ZEE KIN**
**DEPUTY COMMISSIONER**
**FOR PERSONAL DATA PROTECTION**