PERSONAL DATA PROTECTION COMMISSION

[2021] SGPDPC 6

Case No. DP-2004-B6180

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

And

SAP Asia Pte. Ltd.

… *Organisation*

DECISION

SAP Asia Pte. Ltd.

[2021] SGPDPC 6

Lew Chuen Hong, Commissioner — Case No. DP-2004-B6180

30 July 2021

Introduction

1 On 1 April 2020, the Personal Data Protection Commission ("**the Commission**") received a complaint that SAP Asia Pte. Ltd. ("**the Organisation**") had disclosed the payroll information of some of its former employees to the wrong email recipients ("**the Incident**"). The Commission commenced investigations into the Incident thereafter.

Facts of the Case

2 At the material time prior to the Incident, the Organisation had engaged an external vendor ("**the Vendor**") to provide IT solutions for its human resources and payroll system ("**the HR System**"). The Organisation's process of issuing payslips to its employees had been automated as part of the HR System. However, when payslips needed to be issued to individuals who had already left the employment of the Organisation (e.g. final payslips, reimbursements of expenses etc), this could not be done via the HR System. Such payslips needed to be separately generated by the Organisation's human resources department and emailed to the former employees at their personal email addresses. The Organisation was keen to automate the process of issuing payslips to former employees as part of the HR System, and sometime around April 2019, requested the Vendor to develop a new programme within the HR System for this purpose ("**the Programme**").

3 The Organisation had intended to use the Programme to generate and email multiple payslips to multiple former employees simultaneously in one execution of the Programme ("**Multiple Payslip Issuance**"). However, as will be discussed below, this intention was not properly communicated to the Vendor, and the Programme was designed on the incorrect

understanding that only a single payslip would need to be issued to a single employee at a time ("**Single Payslip Issuance**").

4 The Organisation executed the Programme for the first (and only) time on 31 March 2020 to generate and deliver payslips to 43 former employees at their personal email addresses. Believing the Programme to be capable of Multiple Payslip Issuance, the Organisation's representative selected all 43 former employees to be issued payslips in one selection screen of the Programme and executed the process. As the Programme had not been designed to be able to properly execute Multiple Payslip Issuance, this execution of the Programme resulted in 29 out of the 43 former employees receiving their own payslip as well as the payslips of other employees. By way of illustration:

(a) The 1st former employee in the selection received only their own payslip.

(b) The 2nd former employee in the selection received their own payslip as well as the payslip of the 1st former employee.

(c) The 3rd former employee in the selection received their own payslip as well as the payslips of the 1st and 2nd former employees.

5 13 of the 43 former employees had not provided the Organisation with valid email addresses and did not receive any emails with payslips. However, the payslips of these 13 former employees were still generated and disclosed to the 29 other former employees when the Programme was executed on 31 March 2020.

6 In all, the personal data of 43 former employees of the Organisation was improperly disclosed in the Incident. The disclosed personal data comprised each of the former employees':

(a) Name;

(b) NRIC or FIN number;

(c) Employment number;

(d) Bank account number;

(e) Monthly basic salary;

(f) Detailed breakdown of current payment; and

(g) Year-To-Date earnings and deductions.

Remedial actions

7 Following the Incident, as part of remedial actions, the Organisation:

(a) Emailed all 43 former employees on 1 April 2020 informing them about the error and requesting each of them to delete the payslips which were not intended to be emailed to them;

(b) Followed up with the former employees over phone to confirm deletion of the other payslips and received confirmation from 39 of the 43 former employees affected;

(c) Disabled the Programme and reverted to manually generating and emailing payslips to former employees; and

(d) Agreed on continuous process improvements with the Vendor with clear communicated requirements.

Findings and Basis for Determination

Whether the Organisation contravened the Protection Obligation

8 Section 24 of the Personal Data Protection Act 2012 ("**PDPA**") requires an organisation to protect 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 (the "**Protection Obligation**").

9 In this case, the Organisation, a data controller, engaged the Vendor to develop a new feature for its IT systems which processed personal data in its possession (i.e. the Programme). The development of the Programme had obvious implications for the way in which the former employees' personal data would be processed. However, in developing the Programme, the Vendor did not process personal data on behalf of the Organisation and was not the Organisation's data intermediary in this regard. Accordingly, the Protection Obligation in respect of the former employees' personal data was borne solely by the Organisation.

10 In the context of the Programme's development, the Organisation's responsibilities under the Protection Obligation included ensuring that:

(a) The specifications provided to the Vendor accurately reflected the intended use of the IT feature being developed; and

(b) Pre-launch testing of the new feature was accurately scoped to simulate the full range of intended use of the new feature.

11 For the reasons set out below, the Organisation failed both of these responsibilities.

Failure to adequately specify requirements for the Programme

12 It is a data controller's responsibility to ensure that external vendors who are engaged to modify its IT systems know the scope of their work. As stated in *(1) Smiling Orchid (S) Pte Ltd; (2) T2 Web Pte Ltd; (3) Cybersite Services Pte Ltd; (4) East Wind Solutions Pte Ltd* [2016] SGPDPC 19 at [51]:

> " *Data controllers that* (engage) *outsourced service providers have to be clear about the nature and extent of services that the service provider is to provide. There must be a clear meeting of minds as to the services that the service provider has agreed to undertake, and this should be properly documented."*

13 This does not mean that *all* organisations will be expected to be able to give detailed technical instructions to their IT vendors. As clarified in *MDIS Corporation Pte Ltd* [2020] SGPDPC 11 at [14]:

> *"While an organisation may not have — or need to have — the requisite level of technical expertise, a responsible organisation would have engaged competent service providers and made genuine attempts to give proper instructions.* ***The Organisation is only expected to articulate its business requirements as owner of the system, which the service provider can translate into technical requirements****. In addition, as the data controller, the Organisation is required to exercise reasonable oversight to ensure that its instructions are carried out."*
>
> [emphasis added]

14 In previous enforcement decisions, the Commissioner has held organisations in breach of the Protection Obligation for failing to properly communicate business requirements for design changes to IT features:

(a) In *Singapore Cricket Association and another* [2018] SGPDPC 19, the organisation engaged a vendor to redesign its website, including certain pages featuring profiles of its registered players. The organisation's requirements were conveyed to the vendor piecemeal - in meetings, through phone calls, and over text messages. As a result, the vendor misunderstood the intended contents for the player profile pages and incorrectly disclosed around 100 players' personal data including NRIC numbers and contact information as part of the redesigned website.

(b) In *The Central Depository (Pte) Limited & another* [2019] SGPDPC 24, the organisation engaged a vendor to develop software to generate and issue notification letters to its customers. However, the organisation failed to provide the vendor with clear specifications and representative test data that covered the full range of data to be processed and the various processing scenarios. As such, the vendor incorrectly assumed that a particular dataset would always have 4 lines of data

to extract for each letter, when in fact, that dataset could have also had 1, 2, or 3 lines of data. This resulted in a design error that caused the inadvertent disclosure of 1,358 customers' personal data to the wrong recipients when the software was deployed.

(c) In *Horizon Fast Ferry Pte Ltd* [2019] SGPDPC 27, a ferry operator engaged a vendor to redesign its booking website. There was no written contract between the parties, and all instructions and requirements for the redesign were conveyed verbally or over text messages. As a result, the vendor misunderstood the scope of the redesign and incorrectly imported an auto-population feature from one of the organisation's *internal* systems to the redesigned website. This caused the booking form on the redesigned website to automatically populate all fields in the form whenever a passport number that matched an entry in the organisation's passenger database was entered. As a result, the personal data of close to 300,000 of the organisation's passengers was exposed to the risk of unauthorised access.

15 In the present case, the Organisation failed to make clear to the Vendor that the Programme was intended to be used for Multiple Payslip Issuance. This resulted in the Vendor designing the Programme under the wrong impression that all that was required by the Organisation was Single Payslip Issuance.

16 The misunderstanding between the Organisation and Vendor was attributable to the Organisation's instructions in relation to development of the Programme being brief and ambiguous. The Organisation's instructions to the Vendor to were contained in a short service request which read as follows:

"*HI Team,*

Can you please enhance the program (…) *where by when i key in the employee id,* (…) *then*
A template of the email with the payslip is send to the ***selected employee****?*

Thanks!"

[emphasis added]

17 The request only referred to a payslip to be sent to a "*selected employee*" (i.e. in the singular) and not multiple employees (i.e. plural).

18 This reference to using the Programme for a single employee (as opposed to multiple employees) was repeated by the Organisation when later responding to clarifications sought by the Vendor as to why payslips needed to be sent to external email addresses:

> *"HI* (…)*,*
>
> *The sending of email to private address is necessary as we are require to provide payslip to* ***ex employee*** *when ever there is a payment. This is for* ***employee*** *who have left the organization.*
>
> *Thanks!"*

19 Apart from these communications, there was no other documentation of the Multiple Payslip Issuance requirement. If the Organisation intended to use the Programme to send payslips in a single instance to multiple former employees (i.e. Multiple Payslip Issuance) this should have been clearly communicated as a required specification for the Programme. The Organisation's failure to properly communicate its business requirements to the Vendor resulted in the Programme being inadvertently designed in an insecure way.

Failure to carry out adequate user acceptance testing

20 The Organisation's failure to specify Multiple Payslip Issuance as a required functionality of the Programme was compounded by its failure to include any Multiple Payslip Issuance scenarios in its user-acceptance testing ("**UAT**") for the Programme (i.e. testing carried out prior to deploying the Programme for use as part of the HR System).

21 Pre-launch testing is an important means of identifying data protection risks before new IT features are deployed in a live environment, and this has also been emphasised in the

Commission's recently published handbook, *How to Guard Against Common Types of Data Breaches*[1]:

> *"Most organisations fail to recognise that proper testing can help them to identify defects in programming before a system is launched. Sufficient resources should be allocated for testing, and a comprehensive UAT should ensure good test coverage of scenarios including possible user journeys and exception handling.* ***Organisations should also ensure that the planned UAT scenarios match real-world usage.*** *This can be done through a comprehensive gathering of business requirements and identification of relevant usage scenarios by potential users.* ***These should be driven by the business owner.****"*
>
> [emphasis added]

22 In previous enforcement decisions, organisations have been held in breach of the Protection Obligation for failing to properly scope pre-launch testing to simulate real-world use of new IT features:

(a) In *Option Gift Pte Ltd* [2019] SGPDPC 10, the organisation developed a programme to send email confirmations to persons who had made gift redemption requests. The programme was intended to send a single email confirmation to each recipient. However, a coding error meant that while the first email was sent to the first recipient (as intended), the second email was sent to both the first and second recipient and so on (i.e. a similar type of error as in the Incident as described at [4] above). The organisation's UAT was found to be inadequate as the programme had only been tested by sending confirmation emails to the *same* internal email address. There was no testing that simulated the intended use of the programme to send emails to multiple recipients.

(b) In *AIA Singapore Private Limited* [2019] SGPDPC 20, the organisation employed an automated system to generate and send different types of letters to its

[1] https://www.pdpc.gov.sg/news-and-events/announcements/2021/05/handbook-on-how-to-guard-against-common-types-of-data-breaches-now-available

customers. A fix had been deployed to correct an earlier programming error but ended up introducing a further error. When different types of letters were processed in one batch, the further error caused letters to be sent to the wrong recipients. The organisation's testing prior to deploying the fix had only simulated scenarios in which one letter was generated at a time. However, this did not replicate the real-world use of the system as letters were ordinarily generated and dispatched in batches.

(c) In *Grabcar Pte Ltd* [2020] SGPDPC 14, an update deployed for the organisation's mobile application inadvertently exposed the personal data of some users to the risk of unauthorised access by other users. The error arose because the effect of the update on a particular caching mechanism had not been detected in testing. This was partly because the organisation failed to test the update in scenarios where multiple users were accessing the application concurrently (which was a foreseeable real-world scenario).

23 Similar to the above precedents, in the present case, the Organisation's representative only conducted 2 test scenarios as part of UAT, and both only involved Single Payslip Issuance. The failure to test Multiple Payslip Issuance as part of UAT meant that the testing was inadequate to simulate the Organisation's intended use of the Programme, and the Programme's incapability of handling Multiple Payslip Issuance was not picked up at the testing stage as it should have.

24 For the above reasons, the Organisation was determined to have breached the Protection Obligation in respect of the former employees' personal data disclosed in the Incident.

The Commissioner's Directions

25 In determining whether to impose a financial penalty on the Organisation pursuant to section 48J(1) of the PDPA, and if so, the amount of such financial penalty, the factors listed at section 48(6) of the PDPA were taken into account, as well as the following mitigating factors:

Mitigating Factors

(a) The Organisation took prompt remedial actions after being notified of the Incident; and

(b) The Organisation was cooperative during the investigations.

26 Having considered all the relevant factors of this case, the Commissioner hereby requires the Organisation to pay a financial penalty of $13,500 within 30 days from the date of the relevant notice accompanying this 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.

27 No further directions are necessary on account of the remedial measures already taken by the Organisation.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION