PERSONAL DATA PROTECTION COMMISSION

[2022] SGPDPC 5

Case No. DP-2108-B8814

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

And

MyRepublic Limited

… *Organisation*

DECISION

Data Protection *– Protection obligation – Unauthorised access to personal data – Unauthorised disclosure of personal data – Insufficient security arrangements – Failure to implement reasonable access controls – Failure to implement reasonable security controls for cloud environment*

MyRepublic Limited

Lew Chuen Hong, Commissioner — Case No. DP-2108-B8814

5 August 2022

Introduction

1 On 29 August 2021, the Personal Data Protection Commission ("**the Commission**") received information that MyRepublic Limited ("**the Organisation**") had been the subject of a cyber incident. On 1 September 2021, the Organisation informed the Commission that a threat actor had exfiltrated and deleted customers' personal data from its IT systems (the "**Incident**").

2 The Organisation requested for the investigation to be handled under the Commission's Expedited Breach Decision procedure. In this regard, the Organisation voluntarily provided and admitted to the facts set out below, and admitted that it had failed to implement reasonable security arrangements to protect the personal data accessed and exfiltrated in the Incident in breach of section 24 of the Personal Data Protection Act 2012 ("**PDPA**").

Facts of the Case

3 The Organisation is incorporated in Singapore, and is a telecommunications operator that holds a Facilities-Based Operations licence ("**FBO Licence**") under Section 5 of the Telecommunications Act 1999.

4 At the time of the Incident, the Organisation accepted customer orders for mobile services through its Mobile Order Portal ("**Portal**"). The Organisation's customers who applied for mobile services would submit their customer identity verification and number portability documents (the "**KYC documents**") through the Portal, and the Portal would store the KYC documents in a bucket (the "**Bucket**") on cloud-storage procured from Amazon Web Services ("**AWS**").

5 While the Bucket was publicly accessible, its access was restricted through the use of an access key (the "**Access Key**") in the Amazon Identity and Access Management feature. The Access Key could only be used to access the Bucket and no other AWS accounts, systems or bucket used by the Organisation. The Access Key was stored in the source code of the Portal to facilitate the transfer of the KYC documents submitted through the Portal, to the Bucket.

6 On 29 August 2021 (SGT), the Organisation became aware that an external actor had accessed and exfiltrated the KYC documents submitted by customers applying for mobile services. The Organisation received an email from the external actor threatening to publish the downloaded customer data unless a ransom was paid.

7 Following the Incident, the Organisation engaged an IT forensic investigator (among others) to assist in its incident response. Investigations revealed that the external actor had utilised the Access Key to access the Bucket. Fortunately, the compromised Access Key could not be used by the external actor to access the Organisation's other AWS accounts, systems or buckets. However, an unusually large volume of data had been downloaded from the Bucket before it was deleted.

8 While the Organisation was unable to determine with certainty how the external actor had obtained the Access Key, the Organisation determined that the external actor had likely obtained the Access Key through two vulnerabilities identified within the Portal, namely:

(a) The disclosure of the Access Key in the Portal's functionality which displayed technical information; and

(b) The disclosure of the Access Key in the Portal's source code repository which was available to all the Organisation's developers, one of whom may have inadvertently disclosed the Access Key.

9 The personal data of 79,388 of the Organisation's customers was accessed and exfiltrated in the Incident, comprising the following:

(a) For 75,026 Singapore citizens and permanent residents: Scanned copies of both sides of NRIC and work pass cards, which included the customer's full name, address, date of birth, gender, race, place of birth, full NRIC number, photograph, thumbprint, date of issuance of card, (for Employment Passes only) employer and nationality, and (for Dependant's Passes only) nationality;

(b) For 4,362 foreigners: Scanned copies of residential address documents such as utility bill, tenancy agreement or insurance policy, which included the customer's name, address and other information; and

(c) For 3,631 customers porting an existing mobile service: porting form which included the customer's full name and mobile phone number.

(collectively, the "**Customer Data**").

Remedial actions

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

(a) Revoked the Access Key and issued a replacement key for the Bucket;

(b) Removed environment configuration files from the Organisation's Portal that exposed the Access Key;

(c) Reviewed activities across all accounts and buckets to ensure that the compromise was isolated to a single bucket;

(d) Restricted access to buckets to specific IP addresses through a block-all-with exception policy;

(e) Enabled version control on buckets that were not previously controlled/managed;

(f) Reviewed to ensure all buckets are private and in line with AWS' best practices;

(g) Reviewed to ensure all access keys are rotated;

(h) Consolidated all AWS accounts with central monitoring enabled;

(i) Cleaned up DNS registry across the Organisation's IT landscape;

(j) Issued a notification to the affected customers, recommending actions to minimise the risks of identify fraud and social engineering, and offering the affected customers six months of complimentary credit monitoring services;

(k) Conducted dark web monitoring from 3 September 2021 to 3 October 2021 to verify whether the exfiltrated data have been published; and

(l) Commissioned the development of a programme of security improvements for the Organisation's systems in order to reduce the risk of security incidents.

Findings and Basis for Determination

Whether the Organisation had contravened the Protection Obligation

11 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**"). The Organisation is required under the Protection Obligation to implement reasonable security arrangements to prevent the risk of unauthorised disclosure of the Customer Data, notwithstanding that the data was hosted on a vendor's cloud service. This is because the Organisation retains control over such data. In *Commeasure Pte Ltd* [2021] SGPDPC 11 ("***Commeasure***") at [11], the Commission found that even though a vendor was responsible for the security of the cloud infrastructure that it provided to the organisation, the organisation bore ultimate responsibility under the Protection Obligation for making reasonable security arrangements to protect all the customers' data under its control.

12 The reasonableness of the Organisation's security arrangements to protect the Customer Data would be assessed having regard to the volume and sensitivity of such personal data. As stated in the Commission's Advisory Guidelines on Key Concepts in the Personal Data Protection Act (revised 1 October 2021) ("**Advisory Guidelines**") at [17.3], an organisation should design and organise its security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach, and implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity.

13 In the course of its business, the Organisation collected and retained copies of its customers' KYC documents such as NRICs and work passes, which contained their Customer Data, in compliance with its FBO Licence.[1] At the time of the Incident, the Organisation had in its control a high volume of sensitive personal data:

(a) High volume of Customer Data: At the time of the Incident, the Organisation had in its control the Customer Data of almost 80,000 individuals.

(b) Sensitivity of Customer Data: The Customer Data included the customers' full NRIC numbers, photographs, thumbprints, and dates of issuance of their NRIC cards. The sensitivity of such information is heightened and there is an increased risk, for example, of identity theft, as the information could enable access to other services provided by the Government.

14 Accordingly, the Organisation should have implemented stronger security measures to protect the Customer Data.

15 For the reasons set out below, the Organisation failed to put in place such reasonable security arrangements to protect the Customer Data and was determined to be in breach of the Protection Obligation (as also admitted by the Organisation). In particular, the Organisation

[1] Under its FBO Licence, the Organisation is required to (i) maintain a register containing records of its customers, including the customers' identity number such as NRIC number, (ii) make and keep a photocopy of its customers' NRIC, passport or employment pass as evidence of the customers' identity, and (iii) keep the register of the customers for at least 12 months from the date of termination of its services to the customers (among others).

failed to implement sufficiently robust processes to manage the Access Key, and also failed to implement reasonable security controls for its AWS environment.

Failure to implement sufficiently robust processes to manage Access Key

16 The Organisation's Protection Obligation required it to protect the Access Key, which allowed access to the Customer Data in the Bucket. As stated in *Commeasure* at [12], AWS has, in its "Reference Guide – AWS security credentials" ("**AWS Reference Guide**"), advised users to protect the access keys as "anyone who has the access keys for your AWS account root user has unrestricted access to all resources in your AWS account".[2]

17 However, the Organisation failed to implement sufficiently robust processes to protect the Access Key.

18 The Organisation informed the Commission that the Access Key could be disclosed through the Portal's functionality to display technical information, at https://mobile.myrepublic.com.sg/php-info. The functionality, known as "PHP Info", is a standard function of the PHP programming environment and helps programmers to understand the configuration of the environment. The "PHP Info" function is invoked by executing a PHP script file. Thereafter, if the php-info URL is accessed, the browser will display the Portal's operating system environment variable values. These values included the Access Key, which was used by the Portal to access and transfer documents submitted by customers through the Portal to the Bucket. This was a significant vulnerability as anyone who knew or could guess the php-info URL could obtain the Access Key and use it to access the Customer Data in the Bucket. The Organisation also determined that this was the most likely way in which the external actor had obtained the Access Key. The Organisation should not have left the Access Key publicly accessible through the php-info URL. Instead, the Organisation could have disabled the "PHP Info" function or moved the Access Key from the Portal's system environment variables to configuration files available only to authorised parties.

[2] https://docs.aws.amazon.com/general/latest/gr/aws-access-keys-best-practices.html – see "Best practices for managing AWS access keys" (last accessed on 5 August 2022).

19 Further, the Organisation informed the Commission that the Access Key was embedded in the Portal's source code available to all the Organisation's developers via the source code repository. This was another way through which the external actor could have obtained the Access Key or one of the developers with access could have inadvertently disclosed it. The Commission has held in *Commeasure* at [12] that embedding AWS access keys into the source code of applications poses a clear security risk. In the AWS Reference Guide, AWS has likewise cautioned users not to "embed access keys directly into code". The Organisation could have stored the Access Key in a file that is separate from the source code and secured with separate access controls, or it could have utilised third party solutions for the management of access keys.

20 In addition, the Access Key was captured in the clear in mobile order application log files made available to employees, including external developers and engineers, who did not require such information for their functions. If the Organisation wanted to store credentials such as the Access Key in its log files (e.g. for development purposes), it should have implemented reasonable security measures such as a log file redaction mechanism to prevent disclosure of such credentials.

21 In view of the above, the Organisation was found in breach of the Protection Obligation for its failure to implement sufficiently robust processes to manage the Access Key.

Failure to implement reasonable security controls for AWS environment

22 Apart from the Organisation's failures in its management of the Access Key, the Organisation also failed to implement reasonable security controls for its AWS environment.

23 The Commission had stated in the Guide to Data Protection by Design for ICT Systems (2021) ("**Guide**") that as a basic practice, organisations should "[e]nsure that files containing personal data are not accidentally made available on a website or through a web application", and "avoid storing personal data in public folders" (at page 20). In the "Amazon Simple Storage Service – User Guide", AWS has similarly advised its users that "[u]nless [they] explicitly

require anyone on the internet to be able to read or write to [their] S3 bucket, [they] should ensure that [their] S3 bucket is not public".[3]

24 However, as stated at [5] above, the Bucket was publicly accessible. This significantly increased the risk profile of the Bucket as external actors could find the Bucket and thereafter access, exfiltrate and delete the Customer Data in the Bucket, which is what occurred in the Incident. Given the high volume and sensitivity of the Customer Data stored in the Bucket, the Bucket should not have been made publicly available. This is especially if the Bucket was meant to interact only with the Portal for customers to upload KYC documents for retrieval by the Organisation's back-office systems.

25 The Commission had stated in the Guide that organisations should put in place ICT controls to manage data protection risks, including setting appropriate access control rules, access rights, and restrictions for specific user roles (at pages 9 and 15). Access to the Bucket should therefore have been restricted to only authorised applications or users. In this case, the Organisation sought to restrict access to the Bucket through the use of the Access Key, but it turned out to be ineffective because of the Organisation's handling and inadvertent disclosure of the Access Key, as stated above. The Organisation could also have considered layering its defences, and could have supplemented the Access Key with a "block-all but" exception policy that allows only specific IP addresses to access the Bucket, as implemented by the Organisation after the Incident.

26 Accordingly, the Organisation was found to be in breach of the Protection Obligation for failing to implement reasonable security controls for its AWS environment.

The Commissioner's Directions

27 In determining whether to impose a financial penalty on the Organisation pursuant to section 48J(1) of the PDPA, and the amount of any such financial penalty, the matters set out

[3] https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html – see "Amazon S3 Preventative Security Best Practices" (last accessed on 5 August 2022).

at section 48J(1) and the factors listed at section 48J(6) of the PDPA were taken into account, as well as the following mitigating factors:

Mitigating Factors

(a) The Organisation took prompt and effective remedial actions, including notifying the affected individuals; and

(b) The Organisation was cooperative during investigations.

28 The Commission also considered the Organisation's voluntary acceptance of liability for the Incident.

29 Having considered all the relevant factors of this case, the Commissioner hereby requires the Organisation to pay a financial penalty of $60,000 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.

30 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