PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2106-B8421

In the matter of an investigation under section 50(1) of the

Personal Data Protection Act 2012

And

Audio House Marketing Pte Ltd

SUMMARY OF THE DECISION

1. On 1 June 2021, Audio House Marketing Pte Ltd (the "**Organisation**") notified the Personal Data Protection Commission (the **"Commission"**) of a ransomware affecting its customer database (the **"Incident"**). Approximately 98,000 individuals' names, addresses, email addresses and telephone numbers, in the nature of contact information, were affected.

2. The Organisation subsequently requested for this matter to be handled under the Commission's expedited breach decision procedure. This means that the Organisation voluntarily provided and unequivocally admitted to the facts set out in

this decision; and admitted that it was in breach of section 24 of the Personal Data Protection Act (the "**PDPA**").

3. The Organisation's internal investigations revealed that PHP files used to develop a web application on the Organisation's website contained vulnerabilities that allowed the threat actor to carry out a SQL injection attack. The Organisation admitted that it is possible that the vulnerabilities in the PHP files had existed since April 2017, when its website was first launched. Further, even though the Organisation had conducted pre-launch tests prior to the launch of its website, the Organisation admitted that it failed to identify and detect the existing vulnerabilities in the PHP files.

4. SQL injection attacks are well-known vulnerabilities: see "Top Ten" list of the Open Web Application Security Project (OWASP). The Commission has consistently advised organisations to take the necessary precautions to guard against the risk of injection attacks (see para. 15.3 of the Commission's Guide to Securing Personal Data in Electronic Medium, published on 8 May 2015, and revised on 20 January 2017). We note that apart from conducting functionality testing of features such as the shopping cart and payment on its website, the Organisation did not conduct any vulnerability scanning and assessment that would have provided a reasonable opportunity to discover the vulnerabilities in the PHP files that were eventually exploited in the Incident.

5. Compounding the above, the Organisation also did not conduct reasonable periodic security review. A reasonable periodic security review would include

vulnerability scanning and assessments, which would have offered the Organisation the opportunity to detect any vulnerabilities that were not detected during the pre-launch tests, or any vulnerabilities that may have arisen since.

6. Periodic security reviews is also a practice that the Commission has consistently advised organisations to adopt. In our Checklists to Guard against Common Types of Data Breaches, the Commission highlighted that conducting a periodic security review is a basic practice that all organisations ought to embrace. This is also reiterated in para. 6.1(a) of the Commission's Guide to Securing Personal Data in Electronic Medium where we stated that it was a good practice for organisations to "conduct regular ICT security audits, scans and tests to detect vulnerabilities and non-compliance with organizational standards", and Table 13(f) of the same Guide where we encouraged organisations to perform web application scanning and source code analysis to help detect common web vulnerabilities, in particular, those identified in the "Top Ten" list of the OWASP, which includes SQL injection attacks.

7. With the use of IT comes the responsibility for data security in IT systems. We urge organisations who may be unable to conduct such security reviews on their own to engage the necessary expertise from the professionals.

8. Having said that, we note that the Organisation's website was built by a company, which the Organisation's main IT vendor had engaged on the Organisation's behalf. The Organisation did not have any contract with the company that developed the website. As a result, the Organisation failed to stipulate clear job

specifications or any data protection requirements on the company that developed its website. There was also an absence of any data protection requirements in the Organisation's contract with its main IT vendor, who it relied upon to manage and maintain its IT systems. The Commission's published decisions[1] have emphasized that organisations engaging IT vendors should – a) stipulate personal data protection requirements on the vendors, b) make clear the job specifications, especially where they include security maintenance and software updates, and, last but not least, c) exercise reasonable oversight over the vendor responsible for the technical capabilities of the organisation so as to offer adequate protection to the types of personal data that may be affected by the engagement of the vendor. In cases where sub-contracting is contemplated, the Organisation should have identified requirements in its main contract that it requires its main IT vendor to impose similar obligations on and exercise adequate oversight over its sub-contractor.

9. In light of the above, the Organisation is found to have breached the Protection Obligation under section 24(a) of the PDPA.

10. In deciding the appropriate outcome in this case, the Commission considered the Organisation's cooperation throughout the investigation, the Organisation's voluntary admission of breach of the Protection Obligation, and the prompt remediation actions taken. This included disabling the use of its website on the same day of the Incident, reformatting of its webserver, adding security against SQL injections and the implementation of vulnerable assessment and penetration

[1] See Jigyasa [2020] SGPDPC 9 and Civil Service Club [2020] SGPDPC 15

testing. We note that the Organisation managed to restore all the personal data affected without loss, thereby minimizing any disruptions to its operations.

11. Having considered the circumstances set out above and the factors listed at section 48J(6) of the PDPA, the Deputy Commissioner for Personal Data Protection hereby finds the Organisation in breach and directs the Organisation to pay a financial penalty of S$10,000 within 30 days from the notice accompanying date of this decision, failing which interest at the rate specified in the Rules of Court in respect of judgement debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

12. In view of the remedial actions taken by the Organisation, no directions under section 48I are necessary.

The following is the provision of the Personal Data Protection Act 2012 cited in the above summary:

Protection of Personal Data

24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent –

(a) unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.