Determination and Sanction

Inquiry following personal data breach notification by Fresh Dental ("the Controller")

Breach Determination Notice

The Authority is making a determination that Fresh Dental has breached operative provisions of the Data Protection (Bailiwick of Guernsey) Law, 2017 ("the Law"), namely **section 34** relating to *"Duties of controllers in relation to processors"*, and **section 41** relating to *"Duty to take reasonable steps to ensure security".* Details are as follows:

Background to the determination

1. On 25 October 2024, the Authority was made aware of a personal data breach whereby threat actors gained unlawful access to a Fresh Dental employee's Microsoft 365 account ("the account") and subsequently disseminated phishing e-mails from that account to a number of recipients. The same day, Fresh Dental notified the Authority of the breach.

2. The Authority had several concerns in respect of the breach, and Fresh Dental's response to it. As a result, the decision was made to open an inquiry under section 69 of the Law.

Reasons for the determination

Section 34 of the Law

3. Section 34 relates to *"Duties of controllers in relation to processors".*

4. In particular, sub-section 1 provides that:

> *"A controller must not cause or permit a processor to process personal data unless conditions A and B are satisfied."*

Further to this, sub-section 3 states:

> *"Condition B is that there is a legally binding agreement in writing between the controller and the processor setting out –*

(a) the subject matter of the processing,
(b) the duration of the processing,
(c) the nature, scope, context and purpose of the processing,
(d) the category of personal data to be processed,
(e) the categories of data subjects,
(f) the duties and rights of the controller, and
(g) the duties imposed on the processor by sections 35 and 36."

5. The Authority is of the view that Fresh Dental has failed to comply with the requirements of these provisions by virtue of the below:

6. In accordance with the Law, a legally binding agreement must be in place between a controller and processor prior to permitting that processor to process personal data on behalf of the controller. Such agreements are necessary to ensure that the processor is aware of its obligations under the Law, and to outline the scope of processing that the processor is authorised to undertake on behalf of the controller. In essence, while an organisation can outsource certain data processing functions, they cannot outsource their accountability and responsibility for protecting that data.

7. In this case Fresh Dental's IT provider was acting as a processor, processing personal data on behalf of Fresh Dental, during the course of its provision of services. Therefore, a legally binding agreement should have been in place prior to Fresh Dental permitting the IT provider to process personal data on its behalf.

8. When asked to provide a copy of the legally binding agreement in place between Fresh Dental and its IT provider, Fresh Dental confirmed that there was no such agreement. This is despite Fresh Dental having used the provider for approximately eight years, and Fresh Dental stating within its own policies that personal data will only be shared with IT providers under strict data protection agreements.

9. It is understood that, since the initiation of this Inquiry, Fresh Dental has taken steps to implement such an agreement with its IT provider.

Summary

10. In summary:
    - Fresh Dental did not have the necessary legally binding agreement with its IT provider as required by the Law.

Section 41 of the Law

11. Section 41 relates to the "Duty to take reasonable steps to ensure security".

    In particular, sub-section 1 provides that:

    > *"A controller or processor must take reasonable steps to ensure a level of security appropriate to the personal data."*

12. The Authority is of the view that Fresh Dental has failed to comply with the requirements of these provisions by virtue of the below:

13. The Law requires that controllers and processors take reasonable steps to ensure a level of security appropriate to the personal data being processed. These steps may include technical and organisational measures.

14. In determining what steps are reasonable to be taken, a controller or processor must take into account the following factors outlined within section 41(3) of the Law:

    - the nature, scope, context and purpose of the processing,
    - the likelihood and severity of risks posed to the significant interest of data subjects, if the personal data is not secure,
    - best practices in technical measures, organisational measures and any other steps that may be taken, and
    - the costs of implementing appropriate measures.

15. Given that the processing of special category health data is a core activity of Fresh Dental, the measures implemented must be at an elevated level, due to its sensitivity, and reflect the increased potential risk to individuals should the data be compromised.

16. It is understood that this breach occurred as a result of the account being compromised by a threat actor, following a phishing attack. To reduce the risk of accounts being compromised by such attacks, a layered approach of complementary technical and organisational measures should be taken.

17. While some measures had been implemented by Fresh Dental, these measures were not sufficient to prevent compromise. When considering the factors within section 41(3) of

the Law, the Authority considers that additional measures should have been in place including:

- Appropriate employee training
- Measures to detect and reduce the risk of phishing attacks and other similar threats
- Penetration testing

Employee Training

18. Fresh Dental did not provide any employee training relating to cyber security risks, despite it stating within its policies that employees would be trained on recognising cyber threats. Had this training been provided, the likelihood of the employee recognising the signs of a malicious e-mail would have increased, reducing the risk of compromise.

Penetration testing

19. Penetration testing is a method of gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques that might be used by an adversary. The aim of a penetration test is to identify vulnerabilities within a system before the same vulnerability is discovered by a threat actor, allowing the organisation to undertake mitigating action.

20. Prior to the breach, the penetration testing conducted only accounted for one limited element of Fresh Dental's total attack surface and did not target the vulnerabilities that were exploited in this matter.

21. Had Fresh Dental undertaken regular, effective penetration testing, it is likely that vulnerabilities outlined within this report could have been identified and mitigated prior to the breach.

Retention of records (breach investigation concerns)

22. In addition to the concerns regarding the measures that Fresh Dental had in place prior to the breach, the Authority also found that Fresh Dental’s investigation into the breach was insufficient.

23. When an organisation becomes aware of a personal data breach, it must undertake an investigation to identify the extent and root cause of the breach (i.e. specifically what was affected and how and why a breach occurred). This allows the organisation to identify risks posed by the breach and implement appropriate corrective steps to maintain the ongoing security of personal data.

24. Limited records were retained by Fresh Dental of its investigation, meaning that it could not demonstrate that reasonable steps had been taken to ascertain the root cause of the breach.

25. The retention of necessary records for an appropriate period is an important protective measure as it allows:

    - Monitoring of systems and potential early identification of suspicious activities such as unauthorised access to Microsoft 365 accounts.
    - Maintenance of proper audit records regarding access.
    - Performing necessary reviews and risk assessments post-incident.

26. As such, the proper retention of these records, in combination with other supporting systems and processes, can act as both a protective measure (pre-breach) as well as an investigative tool (post-breach).

27. In this case the short retention period was insufficient thereby limiting its ability to properly determine the extent of the breach. By extension, this impacts Fresh Dental's ability to assess their own vulnerabilities and determine appropriate measures that would reduce the risk of reoccurrence.

28. It is noted by the Authority that Fresh Dental did have an incident response plan in place. However, from the lack of records and the evidence submitted to the Authority by Fresh Dental, it is clear that this plan was not followed.

Summary

29. In summary:

    - Fresh Dental failed to undertake reasonable steps to ensure an appropriate level of security of personal data.
    - The investigation undertaken by Fresh Dental in respect of the breach was insufficient: failing to create adequate records of the steps that had been taken to establish the root cause of the breach.

- In addition, Fresh Dental's retention of certain records was insufficient, both as a protective measure and to effectively investigate the breach.
- While Fresh Dental had implemented several policies relating to data protection, these policies were not followed by its employees.

30. This ultimately contributed to the compromise of a staff 365 account, the threat actor gaining unauthorised access to the personal data therein, and allowing them to disseminate further phishing emails to other external accounts, putting additional individuals at risk.

Representations

31. No representations have been received from Fresh Dental.

Sanction

32. When the Authority determines that a controller has breached an operative provision of the Law, it may impose a sanction against that controller as outlined within section 73 of the Law.

33. The Authority hereby issues an enforcement order under section 73(1)(c) of the Law, in respect of Fresh Dental's breach of sections 34 and 41 of the Law. For the purposes of 73(1)(c), subsection (2)(a) will apply, the terms of which are as follows:

1. Fresh Dental must implement reasonable and appropriate technical and organisational measures for its Microsoft 365 accounts, and related systems in order to:

- ***Prevent unauthorised access.***
- ***Detect and provide notification of suspicious authentication activity and unauthorised access.***
- ***Investigate suspicious authentication activity and unauthorised access.***
- ***Remediate suspicious authentication activity and unauthorised access.***

When considering the implementation of said measures, Fresh Dental should take into account section 41(3) of the Law, above.

For clarity, this should include the implementation of training for all relevant staff in cyber security risks, including the identification of potential phishing attacks.

2. ***Fresh Dental must implement a legally binding agreement with their current IT provider or an alternative IT provider, addressing the processing of personal data by both parties, in accordance with section 34 of the Law.***

   We have included links to guidance notes advising Fresh Dental on contracts between controllers and processors – Contracts · ODPA

3. ***Terms 1 and 2 above must be complied with within 3 months of the issuance of a notice under section 73 of the Law. Fresh Dental must provide written confirmation to the Authority within this three-month period that it has complied with terms 1 and 2 of this Order, including a written overview of the measures implemented in compliance with term 1.***

4. ***Within six months of an enforcement order being issued under section 73 of the Law, Fresh Dental must undertake a penetration test of its computer systems. As a minimum, the authentication security of Fresh Dental's Microsoft 365 tenant must be included within the scope of this test.***

   A written overview of the results of this penetration test must be provided to the Authority within the same period.

5. ***Within nine months of an enforcement order being issued under section 73 of the Law, Fresh Dental must consider all recommendations, made following the penetration test required by term 4 of this order, and implement any determined to be reasonable in accordance with section 41 of the Law.***

   Written confirmation of the successful implementation of these recommendations by Fresh Dental must be provided to the Authority within the same period.

   In accordance with section 10 of the Data Protection (General Provisions) (Bailiwick of Guernsey) Regulations, 2018, any records created as a result of the above Order must be retained for a minimum of six years and must be provided to the Authority upon request.

   The Authority will be available should Fresh Dental have any questions regarding compliance with the above terms.