


Case 202100222
Enforcement Order
ADDENDUM

Please note the following:

1. The Enforcement Order in this case identified the data controller as “Betty Boo Real Estate Sales”.
2. At the time of the events described in this Enforcement Order, the registered trade and business license name of the data controller was noted as “Joffer Smith T/A Betty Boo Real Estate Sales”.
3. For clarity, I have now been informed that the registered business name of the data controller has been changed to “Betty Bua T/A Betty Boo Real Estate Sales”.



Sharon Roulstone
Ombudsman

Case 202100222

Enforcement Order

Betty Boo Real Estate Sales

27th April 2023

A. BACKGROUND

- [1] On 10 May 2021, we received a complaint from an individual (the complainant) alleging that the data controller had failed to keep her personal data secure, leading to her being defrauded. She had engaged the data controller's real estate brokerage services via e-mail on 8 March 2021 as she was interested in purchasing property located in Little Cayman. Another real estate company, Tranquil Realty Ltd. (Tranquil), which has a business arrangement with the data controller to co-broker and co-list properties on a 50/50 basis, had listed the property for sale.
- [2] On 9 April 2021, the complainant provided a scanned copy of her passport and proof of address to satisfy the data controller's Know Your Client (KYC) obligations and, in that correspondence, requested that the property owners delay the completion of the sale until August or September to take advantage of a stamp duty exemption. The complainant then signed an offer to purchase agreement for the property, which was sent to the data controller on 10 April. The terms of the agreement required an initial 10% deposit to hold the property.
- [3] On 16 April, the complainant received an e-mail that appeared to be from the data controller. It provided details of a US escrow account for the deposit, to which the funds were wired on 17 April. On 20 April, a further email confirmed receipt of the funds and advised that the property owners required an additional 10-15% deposit to accommodate her request for a delayed closing date, and urged her to provide 10%. The complainant advised that she was not in a position to provide an additional 10% but later agreed to wire 5% after being informed that the property owners threatened to refund her deposit and accept an offer from another buyer.

- [4] On 26 April, the complainant reached out to Tranquil to confirm the legitimacy of the US escrow account details provided to her. She was informed that all closing funds are dealt with only through Tranquil's Cayman Islands bank account. On the same day, the data controller told the complainant that the former's e-mail account had been hacked, and that her previous correspondence had been with fraudsters. The complainant lost a total of KYD\$22,680 (not including wire transfer fees), and subsequently reported the matter to the RCIPS Financial Crimes Unit (FCU) on 27 April.
- [5] Our investigation established that the data controller had first discovered the breach to the email account back in March 2021 when another client had fallen victim to financial fraud when US\$5,500 had been wired to fraudsters in similar circumstances. While a report was made to the RCIPS on 30 March 2021, the data controller had taken no steps to secure her email account at that time, other than to consult with an individual on 28 March 2021 who performed an antivirus scan on the data controller's computer. The complainant stated that she had not previously been made aware that the data controller's e-mail account had been compromised.
- [6] The data controller's business is operated by one person. Due to extenuating personal circumstances, the data controller was unable to co-operate with the Ombudsman at the start of our investigation, leading to significant delays. The response to our requests to undertake an audit to establish the full extent of the breach and provide notifications to the affected data subjects, was also delayed. [Redacted]
- We reiterated our request, after
- which [Redacted] retained the services of Signus Technologies (Signus) to undertake an independent investigation into the email account's breach, and establish the extent to which other data subjects had been impacted.
- [7] The Ombudsman received formal notification of the breach from the data controller on 31 May 2021. The data controller subsequently notified 25 affected data subjects between 25 and 30 August 2021.
- [8] We conducted an extensive investigation under section 43 of the Data Protection Act (DPA), focusing on the technical and organizational measures that were in place at the time of the

breach, and on any mitigating steps that were taken. On 14 April 2022 we provided a copy of our Factual Findings Report to the data controller and its legal counsel, inviting comments by 29 April 2022. No further submissions or comments on the report were received.

Actions taken by the Data Controller

- [9] After the first affected data subject brought the earlier breach to the data controller's attention on 24 March 2021, the data controller consulted with an individual on 28 March 2021, who scanned the computer for threats with antivirus software. However, no further action was taken to secure the e-mail account from the ongoing breach.
- [10] After the complainant informed her of the breach, the data controller took her computer to an electronics store to be assessed. She was told that her e-mail account had been compromised and that an auto-forwarding rule had been found, configured to forward all incoming e-mails to a third party e-mail address. The store removed the auto-forwarding rule and reset her e-mail password.
- [11] The data controller stated that she informed the RCIPS in Cayman Brac who said they would be contacting the FCU in Grand Cayman. However, it appears that the report was not transferred, and on 27 April 2021 the complainant reported the matter directly to the FCU.
- [12] The data controller has since committed to undertake a cyber awareness training course and implemented a new password policy to reset her e-mail account password every two weeks. We would recommend utilising a password locker and implementation of Multi-Factor Authentication (MFA), as a better alternative.

Categories of Personal Data Concerned

- [13] The categories of personal data exposed included each client's first, middle and last name, physical address, e-mail address, a copy of the passport picture page, place of work, and client signature on signed Offer to Purchase forms. While this information is not considered sensitive personal data as defined in section 3 of the DPA, it is sufficient to pose a significant risk of harm to the affected data subjects, if exposed.

B. CONSIDERATION OF ISSUES

a) Whether the data controller had appropriate technical and organisational measures in place before the breach to meet her obligations under the seventh data protection principle.

[14] The seventh data protection principle in the DPA provides:

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

[15] Extensive guidance on this principle, and all other requirements under the DPA, is available on the Ombudsman website.¹

Assessment of Technical Measures

[16] [Redacted]

[17] [Redacted]

¹ Ombudsman, 'Seventh Data Protection Principle – Security – Integrity and Confidentiality', Guide to Data Protection Law 2017 for Data Controllers, <https://ombudsman.ky/data-protection-organisation/data-protection-principles/seventh-data-protection-principle-security-integrity-and-confidentiality>

² Flow Webmail, <https://webmail.candwmail.com/>

[18] [Redacted]

established that the breach likely occurred as a result of a phishing attack on 9 March 2021 and continued until 28 April 2021. [Redacted]

[19] As noted above, an unauthorised mailbox rule had been configured to automatically forward e-mails. [Redacted]

Further checks confirmed that 25 data subjects' personal data had been exposed.

[20] [Redacted]

[21] The recommended authentication standard for safeguarding email accounts from account takeover (ATO) attacks – such as the one in this breach - is to implement strong MFA as part of its core identity and access management framework and implement an e-mail security and password policy that meets industry best practices.³ The [Redacted] in use by the data controller at the time of the breach did not meet this standard.

[22] The data controller bears responsibility under the DPA for ensuring that personal data is processed securely by conducting the necessary due diligence on any e-mail solution used in her business. Such assessments are crucial to determine whether the service provides the highest standard of reliability and security to safeguard business and client data. If the

³ NIST SP 800-63: Digital Identity Guidelines, <https://pages.nist.gov/800-63-3/>

expertise to conduct such assessments is not available in-house, then advice should be procured from a third-party service provider with expertise in this area.

- [23] We contacted the first affected data subject after he received official notification of the personal data breach, in order to obtain further clarity on the incident that ultimately led to his financial losses. It was determined, based on copies of correspondence the first affected data subject provided, and information garnered from Signus' final report, that the threat actors spoofed the e-mail address of another client and, in addition to using that client's identity (full name and e-mail signature details), fraudulently posed as the owner of the property which the first affected data subject intended to purchase. Posing as both the other client and the data controller, the threat actors duped the first affected data subject into wiring US\$5,500 on 9 March 2021, using fraudulent wire transfer instructions provided during e-mail correspondence occurring between 8-10 March 2021.
- [24] It is plain that the data controller did not secure her e-mail account and investigate the full extent of the compromise when the earlier breach was brought to her attention by the first affected data subject on 24 March 2021. The computer was examined by an individual on 28 March 2021, who only scanned the local machine with antivirus software. [Redacted]

Presumably, this service provider had limited expertise in investigating cyber incidents, as he did not investigate the e-mail account or, at the very minimum, reset the e-mail account credentials to stop any further unauthorised access. An opportunity was also missed to secure the audit log files – [Redacted] as noted above – by this service provider and the electronics store who subsequently performed investigatory work and, eventually, reset the account password on 28 April.

Assessment of Organizational Measures

- [25] The data controller had no policies in place governing the processing of personal data within the organisation. Such policies and related employee training play an integral role in ensuring that personal data is being processed in a manner compliant with the DPA.

- [26] In addition to the above, there was no incident response policy or procedure in place to enable the timely detection and response to cyber security incidents and personal data breaches when they occur, and to facilitate compliance with the breach notification requirements in section 16 of the DPA.
- [27] Based on Signus' conclusions in its final report, it is probable that the phishing e-mail, which was the likely source of the breach, was not recognised as such, and a malicious link or attachment was clicked. The data controller confirmed that no previous cyber-security awareness or data protection training had been undertaken before the breach occurred. Such training would have provided the tools and awareness necessary to identify phishing and other malicious e-mails when they reached the data controller's inbox.
- [28] These issues point to a lack of adequate controls to prevent the personal data breach and to respond to it after it had occurred. These gaps left the data controller (and her clients) vulnerable to the breach, which resulted in the exfiltration of an unspecified number of e-mails, of which more than 70 were determined to have contained personal data pertaining to 25 data subjects, including the emails relating to the financial losses suffered by two individuals.
- [29] **In conclusion, the data controller did not meet the requirements of the Seventh Data Protection Principle since personal data was not being processed in a manner that ensured its protection against unauthorised or unlawful processing and against accidental loss, destruction or damage by utilising appropriate technical and organisational measures to ensure a level of security that is appropriate to the risk associated with the processing activities undertaken.**

(b) Whether the data controller complied with section 16 of the DPA when the personal data breach was first brought to her attention on 24 March 2021 and subsequently on 26 April 2021.

- [30] Section 16 in the DPA provides:

(1) In the case of a personal data breach, the data controller shall, without undue delay, but no longer than five days after the data controller should, with the exercise of reasonable diligence, have been aware of that breach, notify the data subject of the data in question and the Ombudsman of that personal data breach, describing –

- (a) the nature of the breach;*
- (b) the consequences of the breach;*
- (c) the measures proposed or taken by the data controller to address the breach; and*
- (d) the measures recommended by the data controller to the data subject of the personal data in question to mitigate the possible adverse effects of the breach.*

(2) A data controller who contravenes subsection (1) commits an offence and is liable on conviction to a fine of one hundred thousand dollars.

[31] Extensive guidance on personal data breaches, and all other requirements under the DPA, is available on the Ombudsman website⁴

[32] Likely due to being unaware of the existence of the DPA and her obligation to comply with its provisions, the data controller did not investigate nor provide formal notification of the personal data breach to the affected data subjects or the Ombudsman when it was first brought to her attention on 24 March 2021. Further, when the complainant again brought this matter to her attention on 26 April 2021, she still did not thoroughly investigate nor provide any formal notifications, even though she apparently informed the complainant in a phone call that she had notified her clients.

[33] After we received the complaint on 10 May 2021, we informed the data controller of her duty to comply with section 16 of the DPA. The data controller then provided the

⁴ Ombudsman, Personal data breaches, Guide to Data Protection Act for Data Controllers, <https://ombudsman.ky/data-protection-organisation/personal-data-breaches>

Ombudsman with two personal data breach notification forms with very little information concerning the incidents. These failed to provide any useful information pertaining to the circumstances of the breach or the mitigation measures taken, which suggests that the full extent of the personal data breach had not been properly investigated at that point.

[34] Not until 5 months later, upon retaining^[Redacted] to act on her behalf, did the data controller undertake all recommended actions to comply with her obligations (albeit far outside the statutory timelines), including thoroughly investigating the breach to the e-mail account and providing compliant notifications to all 25 impacted data subjects.

[35] **Therefore, I conclude that the delay and neglect on the part of the data controller constitutes a failure to comply with section 16(1) of the DPA.**

c) Whether personal data was being processed fairly, in compliance with the data controller's obligations under the first data protection principle.

[36] The first data protection principle in the DPA provides:

Personal data shall be processed fairly.

[37] In addition, the Interpretation of the data protection principles in paragraph 2 of part 2, schedule 1 of the Law states:

First principle: specified information at relevant time

2. For the purposes of the first principle personal data shall not be treated as processed fairly unless the data subject has, as soon as reasonably practicable, been provided with, at a minimum -

(a) the identity of the data controller; and

(b) the purpose for which the data are to be processed.

- [38] Extensive guidance on this principle, and all other requirements under the Law, is available on the Ombudsman website.⁵
- [39] Except in certain limited circumstances, personal data processing is only fair if data subjects have been informed that their personal data will be processed, including how the data will be processed, in accordance with the provision above.
- [40] The data controller’s website did not contain fair processing information in the form of a privacy notice, or in any other format, and the complainant and other users were not provided with such information when they engaged the data controller's real estate services.
- [41] **Therefore, the data controller did not comply with paragraph 2, part 2 of schedule 1 of the DPA as she did not make a privacy notice available to her clients in order to inform her clients of the personal data being processed and the purpose(s) for the processing. Consequently, the data controller breached the first data protection principle of the DPA.**

C. CONCLUSIONS

Findings

- [42] For the above reasons, I make the following findings and decisions:

(a) Seventh data protection principle:

The data controller did not meet the requirements of the seventh data protection principle since personal data was not being processed in a manner that ensured its protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by utilising appropriate technical and organisational measures to ensure an appropriate level of security that is commensurate with the level of risk associated with the processing activities undertaken:

⁵ Ombudsman, ‘First Data Protection Principle – Fair and lawful processing’, Guide to Data Protection Act for Data Controllers, <https://ombudsman.ky/data-protection-organisation/data-protection-principles/first-data-protection-principle-fair-and-lawful-processing>

- I. The technical measures employed by the data controller demonstrated significant weaknesses and vulnerabilities. The data controller employed an email solution which lacked sufficient security controls to protect the account from malicious account takeover attacks, and which was unable to provide audit logs to third-party IT service providers in order to facilitate investigations into cyber incidents when they occurred. Meaningful corrective action was not taken until several weeks after the breach had been brought to the data controller's attention, thereby continuing to expose other users of the service to significant financial and other harms.
 - II. The lack of organizational policies, such as an information security policy, incident response policy, internal privacy and data handling policy were not in place to govern the data controller's information security and data protection obligations which is necessary as part of having appropriate organizational governance in place to prevent unlawful processing. Furthermore, the lack of training with regard to cyber-awareness and data protection contributed to both the occurrence of the breach and the length of time during which it remained unchecked.
- (b) Section 16 – notification:

The data controller did not comply with section 16(1) of the DPA, which requires that data controllers provide notifications to both the Ombudsman and the affected data subjects of the personal data breach in a timely manner.

Even when this obligation was repeatedly pointed out to the data controller, in part due to extenuating circumstances, it still took several more months before proper notifications were communicated.

- (c) First data protection principle – privacy notice:

The data controller did not comply with paragraph 2, part 2 of schedule 1 of the DPA as she did not make a privacy notice available to her clients as soon as reasonably practicable after their data was obtained, in order to inform them of the personal data being processed and the purpose(s) for the processing. Consequently, the data controller breached the first data protection principle of the DPA.

[43] The complainant expressed her desire to seek compensation from the data controller for damages suffered as a consequence of the above contraventions of the DPA. It is her right under section 13 of the DPA to seek such compensation from the data controller in the Grand Court.


Required steps

[44] Under section 45 of the DPA, for the reasons explained above, I require the data controller to take the following steps to bring herself into compliance, as soon as practicable, but in any event, no later than 30 days after this Order is issued:

- (a) In support of the recommendation in Signus' final investigation report, I require that the data controller migrate to a business e-mail solution that supports MFA, industry-standard monitoring and filtering for malicious e-mails, administrative access to audit logs and additional vendor support to facilitate investigations into any future personal data breaches.
- (b) The data controller is required to retain the services of a reputable IT service provider to provide ongoing IT support to her business in order to ensure that she maintains compliance with the seventh data protection principle.
- (c) The data controller is required to undertake cybersecurity awareness training at least annually to improve her ability to identify phishing and other malicious attacks in order to prevent her from falling victim to them in the future. She must also undergo data protection awareness training on an annual basis to ensure that she maintains compliance with the DPA going forward.
- (d) The data controller must develop appropriate policies and procedures to ensure that personal data is safeguarded and to maintain compliance with the provisions of the DPA.

Judicial review

[45] Under section 47, a person who has received an enforcement order under the DPA may, within 45 days of receipt and upon notice to the Ombudsman, seek judicial review of the order to the Grand Court.


Sharon Roulstone
Ombudsman