PDPA PRACTICE

WHAT CONSTITUTES "REASONABLE SECURITY ARRANGEMENTS" UNDER THE PERSONAL DATA PROTECTION ACT

Under section 24 of the PDPA, an organisation, including any individual, company, association, or body of persons, corporate or unincorporated, must protect personal data in its possession or under its control by making "reasonable security arrangements".

*"At the **very basic level**, an overarching personal data protection policy has to be developed and implemented to ensure a **consistent minimum data protection standard** across an organisation's practices, procedures and activities[3]."*

The decisions by the Personal Data Protection Commission (the "Commission") of Giordano Original (S) Pte Ltd ("Giordano") and Carousell Pte Ltd ("Carousell") where both Giordano and Carousell were found *not* to be in breach of Section 24 are both illuminating and instructive as to what constitutes "reasonable security arrangements".

Giordano

On 3 December 2020, the Commission was informed that there was an unauthorised network entry and ransomware infection at the OS and server level that occurred on or about 12 July 2020, resulting in both the personal data of Giordano's employees and members being affected. The unauthorised entry was most likely the result of compromised credentials obtained through phishing. Data affected included names, contact numbers and the partial date of birth of members, and name, NRIC, address, gender, age, contact number, email address, educational and salary information of employees[1].

The Commission's findings

Investigations by the PDPC revealed that Giordano had in place reasonable security measures that are consistent with recommendations made by the Commission. In particular, reference was made to the handbook published by the Commission on "How to Guard Against Common Types of Data Breaches", specifically on preventing malware or phishing attacks.

Giordano had installed and deployed various endpoint security solutions, which was complemented with real-time system monitoring for any internet traffic abnormalities. In addition, Giordano was found to have conducted regular system maintenance, reviews, and updates (such as vulnerability scanning and patching) and had used industry-standard encryption to protect sensitive data. Another point worth mentioning is the implementation of the RSA algorithm, which resulted in the affected personal data being useless to third parties without the decryption key. With no other evidence that the data has been exfiltrated or decrypted, personal data compromising sensitive information was not leaked out.

*"Organisations operating as a group of companies may comply with the Accountability Obligation through binding group-level written policies or intra-group agreements that set **out a common and binding standard** for the protection of personal data across all organisations in the same corporate group. These binding group-level written policies or intra-group agreements are akin to binding corporate rules imposed by an organisation on its overseas recipient of the personal, which oblige the overseas recipient to **provide a standard of protection to the transferred personal data that is at least comparable to that under the PDPA**[4]."*

Further security measures taken by Giordano included the following:

- All documents needed for the designing of data protection systems were properly assessed, reviewed and verified;
- Multiple password policies were imposed, including multi-factor authorisation and periodic changes of passwords;
- Administrative accounts were allocated enhanced protection measures;
- Employees were regularly trained to improve their security awareness;
- Specific persons or teams were assigned to safeguard the security system with clear, designated responsibility which ensured that all data and baseline documents were backed-up for effective data recovery.

The Commission emphasised that it *"endorses the proper use of industry-standard encryption to protect personal data, and will give due weight to organisations which have implemented the recommendations we made in our Handbook in determining whether an organisation has complied with its Protection Obligation under section 24 of the Personal Data Protection Act 2012 (the "PDPA"), or as a strong mitigation factor in the event if the Commission finds that there has been a breach of section 24 of the PDPA."*

Carousell

On 14 May 2021, the Commission was informed of an unauthorised access to the accounts of Carousell's users as a result of credential stuffing. The incident was likely due to threat actor(s) obtaining the login details and passwords of some users due to an exposure of the account details on another service provider's platform. When they have successfully logged into the account, they were able to perform actions as an authorised user, including having access to the data in an individual's account and modifying the account settings[2].

The Commission's findings

Carousell was able to demonstrate that it took prompt actions to mitigate the effects of the data breach and took remedial measures to strengthen the robustness of their security system. It is also important to note that the data breach was the result of credential stuffing (i.e. an attack caused from the

"An organisation will not be taken to have complied with the Accountability Obligation merely because it publishes and communicates a data protection policy to external parties. Any externally communicated data protection policy must be ***given the weight of the necessary internal policies and documented practices*** *to guide an Organisation's employees on how to comply with the PDPA in carrying out their work functions. If no such guidelines or procedures were implemented, this made what was communicated to the Organisation's customers and prospective customers effectively an* ***empty promise*** [5]*."*

automated injection of stolen username and password pairs to gain access to user accounts) and was not because of any inadequate data protection security arrangements.

The Commission found that Carousell had implemented reasonable security arrangements because of the following factors:

- Compromised users accounts were immediately suspended;
- Forced password resets were to be made by all users;
- Suspicious user's accounts were disabled and all suspicious IP addresses were blocked.

Conclusion

Ultimately, there can be no one-size-fit-all solution to what constitutes "reasonable security measures" as every organisation is different. However, the decisions handed down by the Commission are extremely helpful in providing the necessary guidance to every organisation in Singapore to comply with both the letter and spirit of the law.

At **Infinity Legal LLC**, our PDPA Practice, comprising lawyers who are Certified Personal Data Practitioners, aims to provide your organisation with a holistic, yet practical approach to comply with the PDPA. We help clients navigate through the variety of legal issues involving personal data protection.

[1] Personal Data Protection Commission (2021, November 11). No Breach of the Protection Obligation by Giordano. *Personal Data Protection Commission Singapore*
https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Decision--Giordano-Originals-S-Pte-Ltd--151021.ashx?la=en

[2] Personal Data Protection Commission (2021, September 21). No Breach of the Protection Obligation by Carousell. *Personal Data Protection Commission Singapore*
https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Decision---Carousell-Pte-Ltd---030821.ashx?la=en

[3] Personal Data Protection Commission (2022, January 14). Breach of the Protection and Accountability Obligations by Nature Society (Singapore), *Personal Data Protection Commission Singapore.*
https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Decision---Stylez-Pte-Ltd---04082021.ashx?la=en

[4] Personal Data Protection Commission (2021, October 14). Breach of the Protection and Transfer Limitation Obligations by J & R Bossini Fashion, *Personal Data Protection Commission Singapore.*
https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Decision---J--R-Bossini-Fashion-Pte-Ltd---18082021.ashx?la=en

[5] Personal Data Protection Commission (2021, October 14). Breach of the Protection, Accountability and Retention Limitation Obligations by Stylez, *Personal Data Protection Commission Singapore.*
https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Decision---Stylez-Pte-Ltd---04082021.ashx?la=en

CONTACT US

INFINITY LEGAL LLC

无限法律事务所

6 Eu Tong Sen Street
#12-14 The Central
Singapore 059817

www.infinitylegal.com.sg

T: +65 6988 8986
F: +65 6988 8932
E: enquiry@infinitylegal.com.sg