SLAUGHTER AND MAY/

CLIENT BRIEFING

JULY 2023

The PCPD's Softmedia investigation - a cautionary tale with recommendations going forward

INTRODUCTION

The Office of the Privacy Commissioner for Personal Data (the "PCPD") recently completed its investigation into Softmedia[1], finding that it insecurely held personal credit data and improperly retained it. At a time when the PCPD is receiving an increasing number of complaints [2], this investigation serves as a timely reminder of the importance of abiding by the core Data Protection Principles (the "Principles")[3].

THE INVESTIGATION

Background

Softmedia developed systems to provide data referencing and processing services to money lending companies and borrowers. More specifically, it operated a TE Credit Reference System (the "Credit System") through which money lending companies could access credit reference data about borrowers. The Credit System was supposed to be accessible only by those money lending companies to whom borrowers applied for loans via Softmedia's Loan Management System.

This investigation was prompted by the complaint of a data subject who was informed by his lender, that his credit data in the Credit System had been accessed by several other money lending companies with whom the data subject had no dealing.

Was information stored on the Credit System "personal data"?

The credit data for each borrower stored on the Credit System was not viewable against his or her name or HKID Card number (or other personal data) but was instead only shown against a set of code which was derived from an algorithm which transformed the borrower's HKID Card number.

Softmedia argued that there was no personal data on the Credit System because no names, HKID Card numbers or other personal data of borrowers was stored there, and that the process of transforming the HKID Card numbers into the designed codes was "irreversible".

The PCPD nevertheless found that the Credit System stored "personal data" [4], because:

- **Personal identifiers:** Given that individual's HKID Card numbers are inherently unique and fixed and because Softmedia's algorithm generated the same code from the same HKID Card number each time, the codes were "personal identifiers" [5] assigned to individuals by Softmedia for the purpose of their database and uniquely identified individuals.

- **Practicable to identify the data subjects:** When considering a loan application, a money lending company would link information from the Credit System with the personal data stored on the Loan Management System to identify who the borrower is. In fact, in the present complaint, the money lending company acquainted with the borrower was able to identify the complainant's profile on the Credit System by combining the data stored on the two systems to learn that his credit data was accessed by other money lending companies.

Contravention of Principle 4(1) - Security of personal data

The PCPD found that, contravening Principle 4(1), Softmedia failed to take all practical steps to ensure that this personal data stored on the Credit System was protected against unauthorised or accidental access, processing, erasure, loss, or use. The reasons for this conclusion were:

[1] Softmedia Technology Company Limited.

[2] With 11.9% relating to inadequate security of personal data and 5.7% relating to accuracy or retention of personal data according to the PCPD's latest annual report for 2021-2022.

[3] Contained in the Personal Data (Privacy) Ordinance ("the Ordinance").

[4] The Ordinance defines "personal data" as any data (a) relating directly or indirectly to an individual; (b) from which it is practicable for the individual's identity to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable.

[5] The Ordinance defines "personal identifier" as an identifier (a) assigned to an individual by a data user for the purpose of operations of the user; and (b) uniquely identifies that individual in relation to the user but does not include their name. The Ordinance also defines "data" as including a personal identifier.

- According to Softmedia's policy, a money lending company had to obtain a signed authorisation letter from the borrower before accessing any of the credit data stored on the Credit System. However, in reality, money lending companies could freely access the Credit System without complying with these requirements. Softmedia did not appear to have examined or verified that the borrower authorisations were indeed obtained by the money lending companies.

- Softmedia did not monitor and thus did not restrict the number of times that money lending companies could access a codified borrower's credit data on the Credit System. Abnormal access to credit data also went undetected.

- Money lending companies were required to input a password to access the Credit System. However, Softbanks's specific password strength requirements were not enforced and there was no requirement for money lending companies to change their passwords, which even led to a former money lending company employee being able to use the Credit System without permission.

- On receiving valid complaints from borrowers who stated that their data on the Credit System was accessed by unknown money lending companies, Softmedia inadequately penalised the contravening money lending companies.

Contravention of Principle 2(2) - Retention of personal data

The PCPD also found that, contravening Principle 2(2), Softmedia kept personal data on the Credit System indefinitely and accordingly longer than was necessary.

According to the Code of Practice on Consumer Credit Data (the "Code"), a credit reference agency may only retain account repayment data in its database for up to five years[6]. However, the Credit System held over 50,000 credit records where such period was exceeded. Softmedia did not actively delete any credit data after five years had passed.

Consequences for Softmedia

As a result of the above contraventions, the Commissioner served an enforcement notice on Softmedia requiring it to take remedial actions, including deleting credit data in respect of which more than five years had elapsed and formulating policies and measures to restrict access to the Credit System, to verify that borrower authorisations are obtained and to meet the requirements of the Code.

Potential for new regulatory oversight of credit reference databases

The Commissioner also expressed great dissatisfaction that the operation and management of credit reference databases is neither regulated by the industry code nor relevant laws of the financial sector and the code of practice of licensed money lenders.

She recommended that these databases should be regulated or supervised given the "crucial importance", that appropriate penalties are imposed on wrongdoers, that the privacy of borrowers is adequately protected and the security of such databases properly safeguarded. Following this investigation, new regulatory supervision is therefore potentially on the horizon for credit reference databases.

RECOMMENDATIONS AND PRACTICAL TIPS FOR DATA USERS

Recommendations from the Commissioner

In its report, the Commissioner provided specific recommendations for database operators going forward. They were to:

1) Implement a **Personal Data Privacy Management Programme** – to incorporate personal data privacy protection into data users' data governance responsibilities[7].
2) Appoint a **data protection officer** who is responsible for ensuring compliance with the Ordinance and overseeing the implementation of a Personal Data Privacy Management Programme and data protection policies.
3) Engage an **independent compliance auditor** to conduct regular compliance audits on the data users' data management practices.
4) Adopt **stringent penalties for improper use** of systems.

Practical tips for data users on data security and retention

Whilst the investigation concerned a credit reference database, the report should serve to remind all data users of how important it is to protect personal data to prevent unauthorised and improper access to systems and not to retain personal data longer than necessary.

All data users should:

1) **Consider whether the data you control is truly "anonymised" -** If it is still practicable to identify data subjects from anonymised

[6] Five years from either from the date of final settlement of the amount in default or from the date of the individual's discharge from bankruptcy, whichever is earlier.

[7] For further guidance, please refer to the PCPD's "Privacy Management Programme – A Best Practice Guide".

data, ensure that the requirements under the Ordinance are complied with.

2) Put in place effective policies and measures to **verify consent authorisations** by data subjects and **declarations that these have been obtained.**

3) Monitor and detect **abnormal usage or activities** by adopting appropriate measures to capture digital footprints on its websites or databases using audit trails.

4) **Penalise** improper system use detected.

5) Implement **strong password requirements** (e.g. mandating the use of a complex password) and **strong access control** (e.g. requiring regular password changing, using multifactor authentication, and limiting the number of failed log-in attempts).

6) Take all practicable steps to **erase personal data** where it is no longer required for its purpose (subject to limited exceptions)[8].

7) Enhance **employees' awareness of data policies and procedures (e.g. through regular training)**.

CONTACTS

WYNNE MOK
PARTNER
T: +852 2901 7201
E: wynne.mok@slaughterandmay.com

JASON CHENG
ASSOCIATE
T: +852 2901 7211
E: jason.cheng@slaughterandmay.com

London	Brussels	Hong Kong	Beijing
T +44 (0)20 7600 1200	T +32 (0)2 737 94 00	T +852 2521 0551	T +86 10 5965 0600
F +44 (0)20 7090 5000	F +32 (0)2 737 94 01	F +852 2845 2125	F +86 10 5965 0650

Published to provide general information and not as legal advice. © Slaughter and May, 2023.
For further information, please speak to your usual Slaughter and May contact.

www.slaughterandmay.com

[8] For further guidance, please see the PCPD's "Guidance on Personal Data Erasure and Anonymisation".