Inspection Report

(Published under Section 48(1) of the Personal Data (Privacy) Ordinance)

Personal Data System of TransUnion Limited

Report Number： R22 – 0684

Date of Issue： 20 December 2022

Personal Data System of

TransUnion Limited

Section 36 of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (the Ordinance) provides that:-

"*Without prejudice to the generality of section 38, the Commissioner may carry out an inspection of-*

(a) any personal data system used by a data user; or

(b) any personal data system used by a data user belonging to a class of data users,

for the purposes of ascertaining information to assist the Commissioner in making recommendations-

(i) to-

(A) where paragraph (a) is applicable, the relevant data user;

(B) where paragraph (b) is applicable, the class of data users to which the relevant data user belongs; and

(ii) relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the relevant data user, or the class of data users to which the relevant data user belongs, as the case may be."

The term "personal data system" is defined in section 2(1) of the Ordinance to mean "*any system, whether or not automated, which is used, whether in whole or in part, by a data user for the collection, holding, processing or use of personal data, and includes any document and equipment forming part of the system*."

Section 48 of the Ordinance provides that:-

"*(1) ... the Commissioner may, after completing an inspection where section 36(b) is applicable, publish a report-*

(a) setting out any recommendations arising from the inspection that the Commissioner thinks fit to make relating to the promotion of compliance

with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and

(b) in such manner as he thinks fit."

This inspection report is hereby published in the exercise of the powers conferred under section 48(1) of the Ordinance.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
20 December 2022

Table of Contents

Inspection Report

(Published under Section 48(1) of the Personal Data (Privacy) Ordinance)

Personal Data System of

TransUnion Limited

Executive Summary

Background

TransUnion Limited (TransUnion) is a credit reference agency in Hong Kong. On 28 November 2022, TransUnion Credit Information Services Limited, a wholly owned subsidiary of TransUnion, has been appointed as one of the credit reference agencies under the Multiple Credit Reference Agencies Model developed by The Hong Kong Association of Banks, the Hong Kong S.A.R. Licensed Money Lenders Association Limited, and The Hong Kong Association of Restricted Licence Banks and Deposit-taking Companies. According to the information provided by TransUnion, its consumer credit database stores the personal data and credit records of over 5.6 million consumers. Given the sensitivity of consumer credit data, any mishandling or unauthorised access of such data may cause significant financial loss to credit providers and data subjects. In this regard, apart from providing quality service and accurate consumer credit data for credit providers and data subjects, TransUnion as an operator of consumer credit database should also take appropriate security measures to monitor and review the usage of the database persistently in accordance with the requirements of the Personal Data (Privacy) Ordinance (Cap. 486) (the Ordinance) and the "Code of Practice on Consumer Credit Data" (the Code). The purposes of monitoring and reviewing the usage of the consumer credit database are to detect and investigate any

unusual or irregular access or use of consumer credit data, so as to fulfil public expectation and safeguard the personal data system held by TransUnion against any unauthorised or accidental access, processing, erasure, loss and use.

The Office of the Privacy Commissioner for Personal Data (PCPD) carried out an inspection under section 36 of the Ordinance in 2010 to inspect TransUnion's personal data system. TransUnion's compliance with the six Data Protection Principles (DPPs) under the Ordinance and the Code was reviewed and recommendations were made to promote compliance.

With the advancement in technology and the pervasive use of TransUnion's services, there is an ever-increasing public expectation on the data security measures adopted by TransUnion on its consumer credit database. In the circumstance, the Privacy Commissioner for Personal Data (the Commissioner) considers it necessary to review the access control of the consumer credit data system of TransUnion, and the preventive measures and review procedures adopted by TransUnion in monitoring suspicious acts.

The Commissioner therefore decided to invoke the power vested in her under section 36 of the Ordinance to carry out an inspection of the personal data system used by TransUnion (the Inspection). In view of the introduction of multiple credit reference agencies in Hong Kong, the Commissioner considers that the findings and recommendations made as a result of the Inspection would also serve as good reference to other credit reference agencies in ensuring compliance with the requirements of the Ordinance and the Code.

Key Findings

Areas of Good Practices

During the Inspection, the Commissioner was pleased to note that TransUnion had attached great importance to the personal data held by it, and that it set good practices in the following areas:

(i) TransUnion generally embraced the protection of privacy as part of its corporate governance. It implemented the Personal Data Privacy Management Programme (PMP) and appointed a designated officer as the Data Protection Officer (paragraphs 35 & 38).

(ii) TransUnion adopted adequate measures on the protection of personal data in the operation and practices of its consumer credit data system, and the mode of operation conformed with international standards on information security (paragraphs 42-45).

(iii) TransUnion adopted good practices in relation to internal access control of the consumer credit data system, which included setting access rights based on roles, conducting regular reviews of access rights, implementing proper password management, and maintaining detailed staff activity log records. Meanwhile, TransUnion adopted appropriate control measures on credit providers' access to the system through contractual means and carried out constant monitoring and detection of abnormal logins to mitigate the risk of unauthorised access to consumer credit data (paragraphs 47-49).

(iv) TransUnion implemented policies and measures to foster staff awareness on the protection of personal data privacy (paragraphs 52-53).

(v) TransUnion adopted contractual means to prevent unauthorised or accidental access, processing, erasure, loss or use of the personal data transferred to data processors for processing (paragraph 57).

(vi) At the advice of the Commissioner, TransUnion launched a free "Credit Alert Service" in May 2022. TransUnion will alert service subscribers by email whenever there are crucial changes to their credit reports, so that the individuals are aware of the changes in their credit reports and can take early preventive measures or remedial actions (paragraphs 60-61).

(vii) At the advice of the Commissioner, TransUnion also launched a new feature to allow individuals who were victims or suspected victims of doxxing to add remarks to their credit reports, thereby enabling credit providers using the consumer credit reference service of TransUnion (i.e. banks or financial institutions) to be aware of this when reviewing the credit reports and may make reference to that in assessing the individuals' credit applications (paragraph 62).

Areas for Improvement

(i) The Commissioner is of the opinion that TransUnion should update its internal policies and procedures to clearly set out the roles and responsibilities of the Data Protection Officer, and allow him to report directly to the top management (paragraph 38).

(ii) The Commissioner recommends that TransUnion should formulate internal policies and standards that are applicable to TransUnion in Hong Kong based on its global policy, and provide more specific guidance for administrators and users of the consumer credit data system in respect of data retention, use and security. TransUnion should also review regularly whether its local policies are in line with the amendments to the Ordinance, such as making corresponding amendments or updates to its policies after the amendment

provisions of the Ordinance relating to doxxing came into effect in October 2021. The Commissioner notes that after the on-site visits of the Inspection Team, TransUnion committed to formulate internal policies and standards that are applicable to TransUnion in Hong Kong (paragraphs 39-41).

(iii) The Commissioner recommends that TransUnion should standardise the procedures of managing its internal activity log records, specifying the types of data that are recorded, the authority, means and frequency of auditing such records and the follow-up actions that should be taken when suspicious situations are detected. Besides, TransUnion should consider adopting electronic means to assist the reviews for enhancement of accuracy. TransUnion submitted that in response to the Commissioner's recommendation, it is in the process of improving the means and frequency of reviewing its activity log records internally and is considering the use of electronic means to enhance accuracy (paragraph 50).

(iv) The Commissioner recommends that TransUnion should revise its policies relating to suspected abnormal access to specify in detail the investigation and reporting procedures in the event that such access is detected, and to set a reporting deadline that is shorter than the existing policy (which is within two months) for notifying the Commissioner of any suspected abnormal access (paragraph 51).

(v) The Commissioner recommends that TransUnion should incorporate procedures relating to the handling of data breaches into contracts signed with data processors, so that both parties may promptly respond to and take remedial actions on data breach incidents. TransUnion should also conduct a privacy impact assessment on data processors' work practices and procedures before engaging them to handle personal data, so as to analyse the data processing steps and evaluate the associated privacy risks, thus facilitating the introduction of measures that could forestall or mitigate the impact on personal data privacy.

After the appointment of data processors, TransUnion should carry out regular assessment on the data processors' handling of personal data to consider if they have fulfilled the mutually agreed standards, and formulate proper response plans with data processors when unforeseeable privacy risks arise. After the on-site visits of the Inspection Team, TransUnion has adopted the aforesaid recommendation on privacy impact assessment since March 2022 (paragraphs 57-58).

Conclusion

As revealed by the Inspection results, TransUnion has adopted good practices and the security measures of its consumer credit data system are in line with international standards. The Commissioner considers that, in relation to the protection of personal data in its possession, TransUnion complies with the requirements of DPP 4 of Schedule 1 to the Ordinance with regard to the security of personal data. The Commissioner is also pleased to note that TransUnion has accepted the advice of the Inspection Team and implemented a personal data privacy management programme and appointed a Data Protection Officer to institutionalise a proper system for the responsible handling, processing and use of personal data in compliance with the Ordinance. Nonetheless, based on the findings of the Inspection, the Commissioner recommends TransUnion to formulate internal policies and standards which are applicable to TransUnion in Hong Kong based on its global policy, set out the roles and responsibilities of the Data Protection Officer more clearly, standardise the procedures of managing internal activity log records, revise its policies relating to the handling of suspected abnormal access, and conduct regular and timely reviews on the practices of its data processors in handling personal data.

Recommendations

Through the Inspection report, the Commissioner would like to make the following recommendations to organisations handling vast amount of customers' personal data:

(i) **Establish a Personal Data Privacy Management Programme (PMP)**: Organisations should establish and maintain a proper system for the responsible use of personal data in compliance with the Ordinance, and a personal data inventory. A PMP can help organisations comply with the Ordinance, handle data breaches promptly, and gain trust from customers and other stakeholders.

(ii) **Appoint a Designated Officer as Data Protection Officer:** Organisation should set out the roles and responsibilities of the Data Protection Officer, including overseeing the organisation's compliance with the Ordinance and reporting to the top management, as well as incorporating into corporate training materials any data protection issues raised by staff and lessons learnt from data breach incidents involving customers' personal data.

(iii) **Formulate Local Policy:** In addition to global policies in relation to personal data protection (including personal data and information security policies), multi-national organisations should formulate specific local policies based on the local legal framework.

(iv) **Fulfil Corporate Social Responsibility:** Expectations towards corporate behaviour go beyond compliance with legal or regulatory requirements. Organisations should fulfil their corporate social responsibility in their daily operation and commit to enhancing protection towards customers' personal data privacy. Organisations' proactive approach in fulfilling their corporate social responsibility could bring about a win-win outcome for the organisations and their customers, along with long-term competitive edges.

(v) **Monitor Access to Personal Data:** To effectively monitor any suspicious behaviours, organisations should establish a mechanism capable of tracking staff access to personal data, including search and modification records. Organisations should formulate policies that require continuous monitoring to be conducted in a timely and effective manner, and specify follow-up plans and reporting procedures when suspicious situations are detected.

(vi) **Prudently Appoint and Manage Data Processors:** Organisations should conduct privacy impact assessments before engaging data processors to handle personal data on their behalf. The privacy impact assessments assist organisations in analysing the relevant data processing steps and evaluating the associated privacy risks in order to facilitate the introduction of measures that could forestall or mitigate adverse impact on personal data privacy. After the appointment of data processors, organisations should carry out ongoing assessment on the data processors' handling of personal data to consider if they have fulfilled the mutually agreed standards, and formulate proper response plans with data processors when unforeseeable privacy risks arise.

Part I – Background

1. Pursuant to section 8 of the Personal Data (Privacy) Ordinance (Cap. 486) (the Ordinance), the Privacy Commissioner for Personal Data (the Commissioner) shall monitor and supervise compliance with the provisions of the Ordinance, and promote awareness and understanding of, and compliance with, the provisions of the Ordinance, in particular the data protection principles. In this regard, the Commissioner may appoint officers to visit and inspect the premises or activities of a data user involving large-scale collection and use of personal data. The Commissioner may publish the relevant findings for promotion of good practices.

2. TransUnion Limited (TransUnion) is a credit reference agency (CRA) [1] in Hong Kong. On 28 November 2022, TransUnion Credit Information Services Limited, a wholly owned subsidiary of TransUnion, has been appointed as one of the credit reference agencies under the Multiple Credit Reference Agencies Model developed by the Hong Kong Association of Banks, the Hong Kong S.A.R. Licensed Money Lenders Association Limited, and The Hong Kong Association of Restricted Licence Banks and Deposit-taking Companies. According to the information provided by TransUnion, its consumer credit database stores the personal data and credit records of over 5.6 million consumers. Generally speaking, an individual who has applied for credit with

[1] According to clause 1.11 of the "Code of Practice on Consumer Credit Data" (the Code), "CRA" means credit reference agency, which in turn means any data user who carries on a business of providing a consumer credit reference service, whether or not that business is the sole or principal activity of that data user. According to clause 1.9 of the Code, "consumer credit reference service" means the service of compiling and/or processing personal data (including consumer credit scoring), for disseminating such data and any data derived therefrom to a credit provider for consumer credit purposes and, for performing any other functions directly related to consumer credit transactions.

credit providers[2] (e.g. banks) before would have his consumer credit data[3] kept in TransUnion's consumer credit database. TransUnion collects borrowers' consumer credit data, such as credit limits, repayment records and details of default payments, and provides such information for credit providers for their assessment of borrowers' financial status and creditworthiness before deciding whether to grant any credit facilities to reduce credit risk. A consumer credit database is commonly available in credit markets around the world. A good credit record may enable an individual to enjoy better interest rate and terms, and increase the chance of getting a loan application approved.

3. Consumer credit data is protected by the Ordinance. The Commissioner has also issued the "Code of Practice on Consumer Credit Data" (the Code) pursuant to section 12 of the Ordinance to provide practical guidance with respect to the handling of consumer credit data by CRAs and credit providers.

4. Given the sensitivity of consumer credit data, any mishandling or unauthorised access of such data may cause significant financial loss to credit providers and data subjects. In this regard, apart from providing quality service and accurate consumer credit data for credit providers and data subjects, TransUnion as an operator of consumer credit database should also take appropriate security measures to monitor and review the usage of the database persistently in accordance with the requirements of the Ordinance and the Code. The purposes of monitoring and reviewing the usage of the consumer credit database are to detect and investigate any unusual or irregular access or use of consumer credit

[2] Pursuant to clause 1.13 of the Code, "credit provider" means any person described below:
(1) an authorised institution within the meaning of section 2 of the Banking Ordinance (Cap. 155)
(2) a subsidiary of an authorised institution within the meaning of section 2 of the Banking Ordinance (Cap. 155)
(3) a money lender licensed under the Money Lenders Ordinance (Cap. 163)
(4) a person whose business (whether or not the person carries on any other business) is that of providing finance for the acquisition of goods by way of leasing or hire-purchase

[3] Pursuant to clause 1.8 of the Code, "consumer credit data" means any personal data concerning an individual collected by a credit provider in the course of or in connection with the provision of consumer credit, or any personal data collected by or generated in the database of a CRA (including the mortgage count) in the course of or in connection with the providing of consumer credit reference service.

data, so as to fulfil public expectation and safeguard the personal data system held by TransUnion against any unauthorised or accidental access, processing, erasure, loss and use.

5. The Office of the Privacy Commissioner for Personal Data (PCPD) carried out an inspection under section 36 of the Ordinance in 2010 to inspect TransUnion's personal data system. TransUnion's compliance with the six Data Protection Principles (DPPs) under the Ordinance and the Code was reviewed and recommendations were made to promote compliance.

6. With the advancement in technology and the pervasive use of TransUnion's services, there is an ever-increasing public expectation on the data security measures adopted by TransUnion on its consumer credit database. In the circumstance, the Commissioner considers it necessary to review the access control of the consumer credit data system of TransUnion, and the preventive measures and review procedures adopted by TransUnion in monitoring suspicious acts.

7. Section 36 of the Ordinance empowers the Commissioner to carry out an inspection of any personal data system used by a data user or by a data user belonging to a class of data users to assist the Commissioner in making recommendations relating to the promotion of compliance with the provisions of the Ordinance. Given the sensitivity of consumer credit data, the Commissioner therefore decided to invoke the power vested in her under section 36 of the Ordinance to carry out an inspection of the personal data system used by TransUnion (the Inspection).

8. In view of the introduction of multiple credit reference agencies in Hong Kong, the Commissioner considers that the findings and recommendations made as a result of the Inspection would also serve as good reference to other credit

reference agencies in ensuring compliance with the requirements of the Ordinance and the Code.

The Business Structure of TransUnion

9. TransUnion is a CRA and part of the TransUnion Group headquartered in Chicago Illinois, U.S.

10. TransUnion provides services of compiling and/or processing personal data (including consumer credit scoring) for credit providers, including retail banks, credit card issuers, banks' affiliated financial companies, money lenders and other financial institutions. TransUnion also offers consumers the right to access their own consumer credit data at a fee.

11. According to the information provided by TransUnion, there are over 35 million consumer credit accounts and personal data of over 5.6 million data subjects contained in its consumer credit database. Meanwhile, there are over 160 credit providers who have subscribed to TransUnion's consumer credit reference service.

12. During the Inspection, TransUnion had over 140 employees, of which employees from the Consumer Interactive team, Member Engagement & Support Department and Information Technology Department would access and handle consumer credit data in daily operation.

Scope of the Inspection

13. TransUnion, as a data user under the Ordinance, is obliged to comply with the requirements under the Ordinance, including the six DPPs of Schedule 1 to the Ordinance, in respect of data collection, retention, use, and security of personal

data in its consumer credit database. The six DPPs are reproduced at **Appendix A**.

14. The Inspection focused on the security measures in relation to access control of the consumer credit data system adopted by TransUnion. In respect of security of personal data, DPP 4(1) requires that all practicable steps shall be taken to ensure that any personal data held by a data user is protected against unauthorised or accidental access, processing, erasure, loss or use having particular regard to –

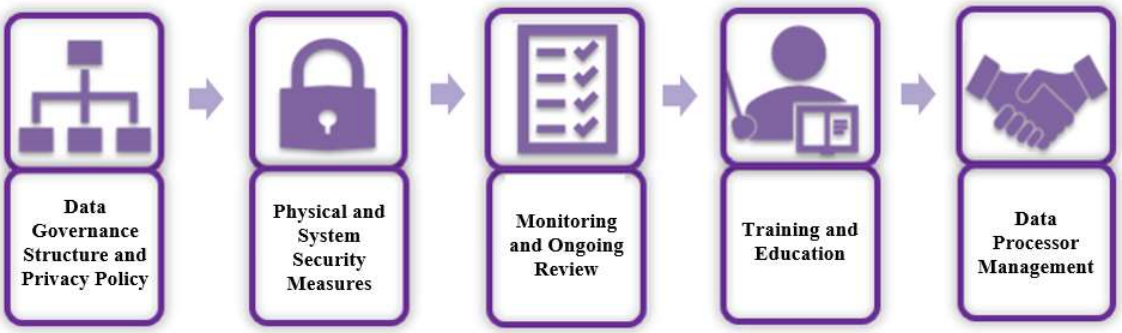
(a) the kind of data and the harm that could result if any of those things should occur;
(b) the physical location where the data is stored;
(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;
(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
(e) any measures taken for ensuring the secure transmission of the data.

15. Pursuant to DPP 4(2), if a data user engages a data processor[4] to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

16. Clause 3.11 of the Code on "data security and system integrity safeguards by CRA", which covers measures to be taken in preparation for providing consumer credit reference service, measures to be taken in daily operations, and log of access by credit providers, is relevant to the Inspection. The relevant clauses of the Code are reproduced at **Appendix B**.

[4] whether within or outside Hong Kong

17. Having considered the amount and nature of personal data handled by TransUnion, the Commissioner defined the main scope of assessment on the policies and practices of TransUnion's consumer credit data system as follows:



Part II – Methodology

18. After informing TransUnion of the Commissioner's intention to carry out the Inspection, a pre-inspection meeting was held between the Inspection Team[5] and representatives of TransUnion headed by their Managing Director in Hong Kong. At the meeting, the Inspection Team explained the purpose of the Inspection and obtained information about the operation and workflow of the consumer credit data system of TransUnion.

19. In order to inspect the consumer credit data system of TransUnion and how its staff members and credit providers effectively comply with TransUnion's data security policies and practices, the Inspection Team obtained from TransUnion all relevant policies, manuals, guidelines, employees' code of conduct, training materials, and service contracts between TransUnion and data processors for examination.

20. Besides, the Commissioner exercised her power of entry on premises under the Ordinance to conduct on-site visits. In September 2021, with the agreement of all parties concerned, the Inspection Team conducted six visits to TransUnion's head office, customer service centre, data centres and call centre.

21. The Inspection Team's work during those on-site visits included:

    (i) Face-to-face interviews with responsible personnel for the management of the consumer credit data system (including staff members of TransUnion and its agents);

[5] The Inspection Team was composed of one Chief Personal Data Officer, one Senior Personal Data Officer and two Personal Data Officers.

(ii) Visits to different departments of TransUnion to examine the actual operation of the consumer credit data system and the relevant access control mechanisms;

(iii) Observation on TransUnion's demonstration on the operation of its consumer credit data system, the workflow of accessing personal data from the system, and the management procedures on staff access control of personal data; and

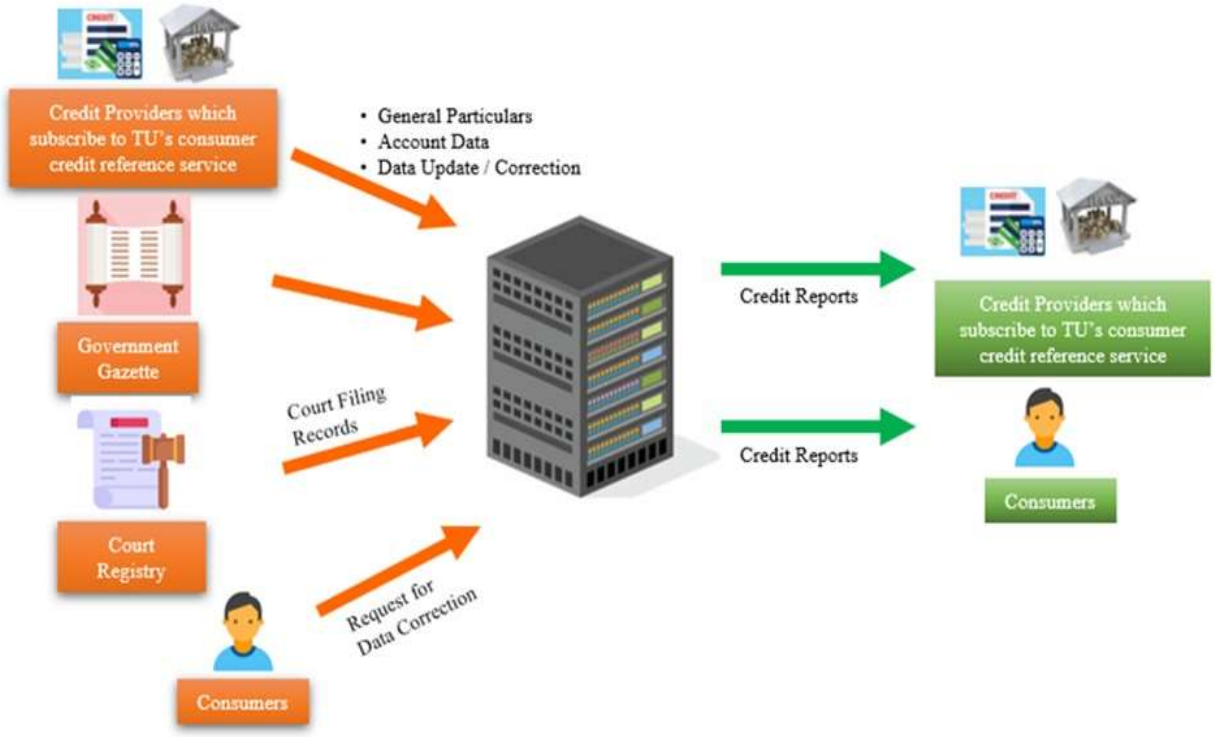
(iv) Random check on TransUnion's paper and computer records containing consumer credit data, including the staff activity log records in the consumer credit data system.

22. The Inspection Team also arranged a mystery customer to visit TransUnion's customer service centre in order to gain a thorough understanding of how TransUnion handled an individual's application for credit report.

Part III – Consumer Credit Data System of TransUnion

23. TransUnion as a data user should comply with the requirements under the Ordinance. At the same time, TransUnion is a CRA in Hong Kong and should observe the relevant requirements under the Code. Aside from legal proceedings, a failure to observe the Code by a data user will weigh unfavourably against the data user in any case brought before the Commissioner.

24. The flow of personal data collection and use in TransUnion's consumer credit data system[6] is as follows:



Consumer Credit Data System of TransUnion

[6] TransUnion has put a few independent systems in place to handle consumer credit data.

Collection of Consumer Credit Data

25. According to clauses 3.1.1 to 3.1.8 of the Code, TransUnion may collect individuals' personal data for the purpose of providing consumer credit reference service. The consumers' personal data held by TransUnion comes from three major sources:

- Credit providers using TransUnion's consumer credit reference service (such as banks, finance companies and credit card companies);
- Public records; and
- Consumers.

26. A credit provider who has collected consumer credit data from an individual in relation to a non-mortgage account[7] or a mortgage account[8] may thereafter provide TransUnion with the relevant consumer credit data according to clause 2.4 of the Code. There are two ways for credit providers who have subscribed to TransUnion's consumer credit reference service to supply consumer credit data to TransUnion's consumer credit data system, namely on-line contribution for data pertaining to a single consumer, and batch contribution for data pertaining to multiple consumers. Upon receipt of the consumer credit data, TransUnion will update the consumer credit data of the relevant individuals.

[7] Consumer credit data collected in relation to a non-mortgage loan include name, address, contact information, date of birth, Hong Kong Identity Card number or travel document number, credit application data not related to a mortgage loan (being the fact that the individual has made an application for consumer credit, the type and the amount of credit sought) and credit card loss data.

[8] Consumer credit data collected in relation to a mortgage loan include name, capacity (i.e. whether as borrower, mortgagor or guarantor), Hong Kong Identity Card number or travel document number, date of birth, address, account number, type of the facility, account status (active, closed, write-off, etc.), account closed date and mortgage application data.

27. TransUnion will collect individuals' data from public records, including any action for the recovery of a debt or judgments for monies owed entered against the individuals, any declaration or discharge of bankruptcy that are available in the Government Gazette and civil actions in the Court Registry. Individuals may also submit an application to TransUnion for correction of their personal data.

Use of Consumer Credit Data

28. A credit provider who has subscribed to TransUnion's consumer credit reference service can make enquiries on credit reports through the following ways:

- Host to host enquiry: Enquiry via a dedicated lease line between the credit provider and TransUnion; and

- PC online enquiry: Login to TransUnion's system dedicated to credit providers for enquiry.

29. Consumer credit data is also provided for individuals in the form of credit reports upon request. Individuals may obtain their credit reports in person at TransUnion's customer service centre by appointment or through TransUnion's online system at a fee.

30. A typical credit report of an individual contains the following information:

- Personal data: name, identification document number, date of birth, addresses and telephone numbers, etc.;

- Credit activities: credit usage and repayment history, etc.;

- Public records: litigation relating to recovery of debt, bankruptcy and winding-up petitions;

- Enquiry records: members' review records within the last two years; and
- Credit score: a numerical snapshot of the credit report.

Part IV – Key Findings

31. This report is based on the information provided by TransUnion and the matters that came to the Inspection Team's attention during on-site visits. The legal obligation to comply with the requirements under the Ordinance and the Code rests with TransUnion. The findings and recommendations made in this report do not in any way affect or prejudice the Commissioner in exercising any powers or performing any functions under the Ordinance.

32. In respect of security of personal data, DPP 4(1) requires that all practicable steps shall be taken to ensure that any personal data held by a data user is protected against unauthorised or accidental access, processing, erasure, loss or use. Pursuant to DPP 4(2), if a data user engages a data processor[9] to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

33. This report evaluates the personal data protection aspects as described in paragraph 17. Apart from highlighting the possible areas of improvement, this report also demonstrates the good practices adopted by TransUnion in safeguarding the consumer credit data it holds.

(I) Data Governance Structure and Privacy Policy

Personal Data Privacy Management Programme

34. The Commissioner has been advocating for organisations to develop their own Personal Data Privacy Management Programme (PMP) and appoint a Data

[9] whether within or outside Hong Kong

Protection Officer to institutionalise a proper system for the responsible use of personal data in compliance with the Ordinance[10].

35. The Commissioner considers that TransUnion generally embraced the protection of privacy as part of its corporate governance. That said, given the size of the consumer credit data system TransUnion manages, and the volume and sensitivity of the personal data it processes, the Commissioner recommends that TransUnion should construct and implement its PMP in a more comprehensive manner.

36. Based on a set of standard operating procedures applicable to TransUnion in Hong Kong with effect from June 2021 provided by TransUnion, the role of Data Protection Officer was taken up by a Regional Compliance Head. The said document only described the role of the Data Protection Officer briefly, including basic requirements on offering independent advice and oversight to TransUnion in respect of data protection matters, and ensuring provision of data protection guidance and training to employees at regular intervals.

37. The Commissioner considers the role of the Data Protection Officer described in the standard operating procedures rather superficial, as it failed to specify the responsibilities, scope of work and the reporting relationships with other personnel. No detailed description on the role of the Data Protection Officer could be found in other personal data privacy policies and relevant documents submitted by TransUnion.

38. Considering the vast amount of consumer credit records maintained by TransUnion, the Commissioner is of the opinion that TransUnion should appoint a designated officer as the Data Protection Officer to oversee compliance with the Ordinance and the Code, implement the PMP, and update

[10] For examples and practical guidance on how to devise and implement a comprehensive PMP, please refer to the Best Practice Guide on Privacy Management Programme: https://www.pcpd.org.hk//chinese/resources_centre/publications/files/PMP_guide_c.pdf

its internal policies and procedures to clearly set out the roles and responsibilities of the Data Protection Officer, and allow him to report directly to the top management. The Commissioner is pleased to note that TransUnion subsequently informed the PCPD that it has implemented the PMP and appointed a designated officer as the Data Protection Officer.

Local Privacy Policy

39. The Commissioner recognises that TransUnion, as part of the TransUnion Group in the U.S., is obliged to comply with the global policies established by its headquarters, including personal data protection and information security policies.

40. The Inspection Team noted that for some of the policies relating to the protection of personal data, TransUnion only maintained global policies formulated by its headquarters. Such policies might not be fully compatible with TransUnion's actual operation in Hong Kong in all circumstances. For example, the activity log management policy formulated by the headquarters clearly specified the data retention period and audit frequency; however, the Inspection Team found that TransUnion's practices of managing individual systems which contained consumer credit data in this regard deviated from the policy of the headquarters, and such practices was not documented in any policies applicable in Hong Kong.

41. The Commissioner recommends that TransUnion should formulate internal policies and standards that are applicable to TransUnion in Hong Kong based on its global policy, and provide more specific guidance for administrators and users of the consumer credit data system in respect of data retention, use and security. TransUnion should also regularly review whether its local policies are in line with the amendments to the Ordinance, such as making corresponding amendments or updates to its policies after the amendment provisions of the Ordinance relating to doxxing came into effect in October

2021. The Commissioner notes that after the on-site visits of the Inspection Team, TransUnion committed to formulate internal policies and standards that are applicable to TransUnion in Hong Kong.

(II) Physical and System Security Measures

42. The Inspection Team reviewed the physical and system security measures protecting personal data during on-site visits. Owing to the confidentiality of the security measures, the details are not revealed in this report. Nevertheless, the Inspection Team noted that TransUnion has classified consumer credit data as "confidential", which must be carefully stored, used and disposed of. TransUnion has also complied with International Organisation for Standardization (ISO) standards when formulating its information technology security policy for enhancing its defence in data security. The policy covers technical areas such as system protection, access control, physical security.

43. The Commissioner was also pleased to note that TransUnion had been making ongoing efforts to strengthen its data security control measures, adopting the ISO standards to establish, implement, maintain and constantly enhance its control measures in information security, so as to reduce the risk to data privacy.

44. From 2003 to 2021, TransUnion engaged independent auditors to conduct annual privacy compliance audits on its personal data system to assess the system integrity, accuracy and security level.

45. In general, the Commissioner considers that TransUnion adopted adequate measures on the protection of personal data in the operation and practices of its consumer credit data system. In particular, the Commissioner is pleased to note that TransUnion's mode of operation conformed with international standards on information security.

(III) Monitoring and Ongoing Review

46. Having considered the business nature of TransUnion, in particular the vast amount of consumer credit data in TransUnion's consumer credit database and the sensitive nature of such data, the Commissioner considers that TransUnion should continue monitoring the usage of its consumer credit data system and reviewing staff activities in the system. The Commissioner is delighted to note that TransUnion has standard policies to notify staff clearly of its monitoring activities on their use of corporate devices and systems.

TransUnion's Internal Access Control

47. TransUnion adopted good practices in relation to internal access control of the consumer credit data system as follows:

- **Setting Access Rights based on Roles:** Access was granted on a "need-to-know" basis commensurate with the ranks, roles and responsibilities of staff members.

- **Conducting Regular Reviews of Access Rights:** Written approval must be obtained before granting any access right to individual staff members. TransUnion has a system in place to regularly remind department heads to review and update the access right of individual staff members of their departments.

- **Implementing Proper Password Management:** TransUnion established policies prohibiting any sharing of passwords and requiring passwords to be changed on a regular basis. Passwords must fulfil the minimum length and complexity requirements. A user account will be locked after repeated incorrect login attempts.

- **Maintaining Detailed Staff Activity Log Records:** In addition to keeping staff activity log records regarding its consumer credit data system, TransUnion also conducts regular reviews on the activity log records to check for any abnormal data access.

TransUnion's Access Control on Credit Providers

48. TransUnion possesses a massive database of consumer credit data. For business operation purpose, credit providers need to obtain individuals' consumer credit data for assessing the risk of approving individual credit applications, preventing frauds and recovering debts. According to the information provided by TransUnion, there are over 160 credit providers who have subscribed to TransUnion's consumer credit reference service.

49. The Inspection Team noted that TransUnion adopted appropriate control measures on credit providers' access to the system through contractual means and carried out constant monitoring and detection of abnormal logins to mitigate the risk of unauthorised access to consumer credit data.

The Commissioner's Recommendations regarding the Areas of Improvement on TransUnion's Access Control

50. The Inspection Team also noted that there was a lack of consistency on the frequency and means of reviewing the activity log records among different departments within TransUnion, which reflected that TransUnion did not have any unified standard in this regard. Besides, TransUnion conducted reviews on internal activity log records manually without the assistance of any electronic means. Given the vast amount of the internal activity log records, the Commissioner recommends that TransUnion should standardise the procedures of managing its internal activity log records, specifying the types of data that are recorded, the authority, means and frequency of auditing such records and the follow-up actions that should be taken when suspicious situations are

detected. Besides, TransUnion should consider adopting electronic means to assist the reviews for enhancement of accuracy. In response to the Commissioner's recommendation, TransUnion submitted that it is in the process of improving the means and frequency of reviewing its activity log records internally and is considering the use of electronic means so as to enhance accuracy.

51. In addition, in case of any suspected abnormal access[11] by a credit provider, TransUnion should report such suspected abnormal access as soon as reasonably practicable to the senior management of the credit provider and to the Commissioner according to the Code. PCPD's records show that TransUnion only reported a case of suspected abnormal access to the Commissioner nine months after the incident. The Commissioner notes that TransUnion has put in place a policy to handle suspected abnormal access since 2020, which stipulates that TransUnion would normally report any suspected abnormal access as stipulated in the Code to the Commissioner together with the credit providers' written explanation within two months. The Commissioner recommends that TransUnion should revise its policies relating to suspected abnormal access to specify in detail the investigation and reporting procedures in the event that such access is detected, and to set a reporting deadline that is shorter than the existing policy (which is within two months) for notifying the Commissioner of any suspected abnormal access.

(IV) Training and Education

52. TransUnion implemented policies and measures to foster staff awareness on the protection of personal data privacy. These include providing all employees induction training on data protection, providing continuous training on personal

[11] The occurrence of access on five or more occasions within a period of 31 days made by the same credit provider seeking access to the consumer credit data of a particular individual held by a CRA, in connection with the review of existing consumer credit facilities pursuant to clause 2.9.1.2, 2.9A.2, 2.9A.4, 2.9A.5, 2.10A.2 , 2.10A.3 or 2.10A.4 of the Code.

data protection through an internal electronic platform, and regularly disseminating information security tips to staff through email by the Information Security Department.

53. During on-site visits, the Inspection Team was aware that TransUnion had displayed tips on the protection of personal data privacy in the office area as shown below:

(V) **Data Processor Management**

54. It has become increasingly common for data users to outsource and entrust their personal data processing work to agents. Data breaches may occur if insufficient steps are taken by the outsourced parties (data processors[12]) to protect the personal data entrusted to them, and may cause substantial and irrecoverable damage to the affected data subjects.

55. Pursuant to DPP 4(2), if a data user engages a data processor[13] to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

56. The Inspection Team noted that TransUnion had outsourced and entrusted personal data processing work to third-party service providers, including service providers responsible for operating the call centre and data centres, and a security company responsible for transmitting and storing backup tapes.

57. The Commissioner considers that TransUnion adopted contractual means to prevent unauthorised or accidental access, processing, erasure, loss or use of the personal data transferred to data processors for processing. Nonetheless, the Commissioner recommends that TransUnion should incorporate procedures relating to the handling of data breaches into contracts signed with data processors, so that both parties may promptly respond to and take remedial actions on data breach incidents.

---

[12] A "data processor" is a person who processes personal data on behalf of another person and does not process the data for any of the person's own purposes. Data processors are not directly regulated under the Ordinance. Instead, if a data user engages a data processor to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data, and to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

[13] whether within or outside Hong Kong

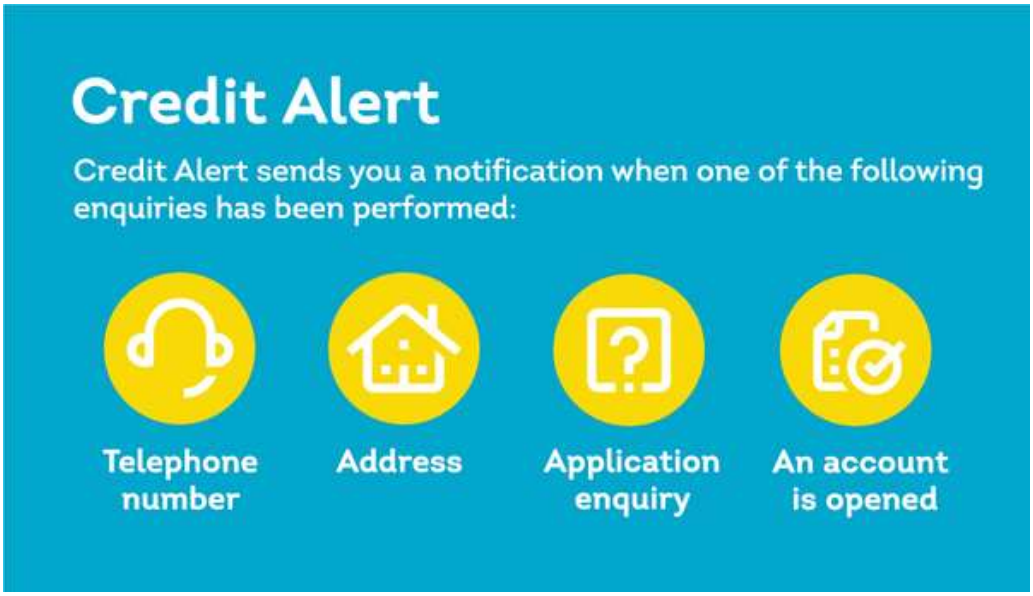
58. The Commissioner also recommends that TransUnion should conduct a privacy impact assessment on data processors' work practices and procedures before engaging them to handle personal data, so as to analyse the data processing steps and evaluate the associated privacy risks, thus facilitating the introduction of measures that could forestall or mitigate the impact on personal data privacy. After the appointment of data processors, TransUnion should carry out regular assessment on the data processors' handling of personal data to consider if they have fulfilled the mutually agreed standards, and formulate proper response plans with data processors when any unforeseeable privacy risks arise. The Commissioner is pleased to note that after the on-site visits of the Inspection Team, TransUnion has adopted the aforesaid recommendation on privacy impact assessment since March 2022.

(VI) **Further Data Protection Measures**

59. Expectations of corporate behaviours go beyond compliance with legal or regulatory requirements. While striving for operational results, organisations should also fulfil its corporate social responsibility.

Free Credit Alert Service

60. During the Inspection, TransUnion offered a "Credit Alert Service" to registered individuals and its monthly subscribers. If there are crucial changes to the credit reports of the individuals (see below), such as a new enquiry or account created, TransUnion will send the individuals concerned emails and/or message notifications.



Source: https://www.transunion.hk/product/credit-report

61. TransUnion demonstrated its understanding of the public's rising expectation on the protection of personal data privacy. During the Inspection, at the advice of the Commissioner, TransUnion launched a free "Credit Alert Service" in May 2022. Members of the public who have successfully authenticated themselves via TransUnion's website can subscribe to the free "Credit Alert Service" without purchasing any credit report. TransUnion will alert service subscribers by email whenever there are crucial changes to their credit reports (as shown above), so that the individuals are aware of the changes in their credit reports and can take early preventive measures or remedial actions.

Inclusion of Remarks in Credit Reports

62. During the Inspection, TransUnion told the Inspection Team that it had taken note of the serious doxxing acts taking place since mid-2019, and the disclosure of personal data of a significant number of individuals in the public domain or on social platforms. Some of the personal data of the victims of doxxing was used for unlawful purposes, including the making of loan applications. In light of that and at the advice of the Commissioner, TransUnion launched a new

feature to allow individuals who were victims or suspected victims of doxxing to add remarks to their credit reports, thereby enabling credit providers using the consumer credit reference service of TransUnion (i.e. banks or financial institutions) to be aware of this when reviewing the credit reports and may make reference to that in assessing the individuals' credit applications.

Conclusion

63. As revealed by the Inspection results, TransUnion has adopted good practices and the security measures of its consumer credit data system are in line with international standards. The Commissioner considers that, in relation to the protection of personal data in its possession, TransUnion complies with the requirements of DPP 4 of Schedule 1 to the Ordinance with regard to the security of personal data. The Commissioner is also pleased to note that TransUnion has accepted the advice of the Inspection Team and implemented a personal data privacy management programme and appointed a Data Protection Officer to institutionalise a proper system for the responsible handling, processing and use of personal data in compliance with the Ordinance. Nonetheless, based on the findings of the Inspection, the Commissioner recommends TransUnion to formulate internal policies and standards which are applicable to TransUnion in Hong Kong based on its global policy, set out the roles and responsibilities of the Data Protection Officer more clearly, standardise the procedures of managing internal activity log records, revise its policies relating to the handling of suspected abnormal access, and conduct regular and timely reviews on the practices of its data processors in handling personal data.

Part V – Recommendations

64. Through the Inspection report, the Commissioner would like to make the following recommendations to organisations handling vast amount of customers' personal data:

(i) **Establish a Personal Data Privacy Management Programme (PMP)**: Organisations should establish and maintain a proper system for the responsible use of personal data in compliance with the Ordinance, and a personal data inventory. A PMP can help organisations comply with the Ordinance, handle data breaches promptly, and gain trust from customers and other stakeholders.

(ii) **Appoint a Designated Officer as Data Protection Officer:** Organisation should set out the roles and responsibilities of the Data Protection Officer, including overseeing the organisation's compliance with the Ordinance and reporting to the top management, as well as incorporating into corporate training materials any data protection issues raised by staff and lessons learnt from data breach incidents involving customers' personal data.

(iii) **Formulate Local Policy:** In addition to global policies in relation to personal data protection (including personal data and information security policies), multi-national organisations should formulate specific local policies based on the local legal framework.

(iv) **Fulfil Corporate Social Responsibility:** Expectations towards corporate behaviour go beyond compliance with legal or regulatory requirements. Organisations should fulfil their corporate social responsibility in their daily operation, and commit to enhancing

protection towards customers' personal data privacy. Organisations' proactive approach in fulfilling their corporate social responsibility could bring about a win-win outcome for the organisations and their customers, along with long-term competitive edges.

(v) **Monitor Access to Personal Data:** To effectively monitor any suspicious behaviours, organisations should establish a mechanism capable of tracking staff access to personal data, including search and modification records. Organisations should formulate policies that require continuous monitoring to be conducted in a timely and effective manner, and specify follow-up plans and reporting procedures when suspicious situations are detected.

(vi) **Prudently Appoint and Manage Data Processors:** Organisations should conduct privacy impact assessments before engaging data processors to handle personal data on their behalf. The privacy impact assessments assist organisations in analysing the relevant data processing steps and evaluating the associated privacy risk in order to facilitate the introduction of measures that could forestall or mitigate adverse impact on personal data privacy. After the appointment of data processors, organisations should carry out ongoing assessment on the data processors' handling of personal data to consider if they have fulfilled the mutually agreed standards, and formulate proper response plans with data processors when unforeseeable privacy risks arise.

Appendix A

Personal Data (Privacy) Ordinance

Schedule 1

[ss. 2(1) & (6)]

Data Protection Principles

1. Principle 1—purpose and manner of collection of personal data

(1) Personal data shall not be collected unless—

(a) the data is collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;

(b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and

(c) the data is adequate but not excessive in relation to that purpose.

(2) Personal data shall be collected by means which are—

(a) lawful; and

(b) fair in the circumstances of the case.

(3) Where the person from whom personal data is or is to be collected is the data subject, all practicable steps shall be taken to ensure that—
(Amended 18 of 2012 s. 40)

(a) he is explicitly or implicitly informed, on or before collecting the data, of—

(i) whether it is obligatory or voluntary for him to supply the data; and

(ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and

(b) he is explicitly informed—

(i) on or before collecting the data, of—

(A) the purpose (in general or specific terms) for which the data is to be used; and

(B) the classes of persons to whom the data may be transferred; and

(ii) on or before first use of the data for the purpose for which it was collected, of— *(Amended 18 of 2012 s. 40)*

(A) his rights to request access to and to request the correction of the data; and

(B) the name or job title, and address, of the individual who is to handle any such request made to the data user, *(Replaced 18 of 2012 s. 40)*

unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data was collected and that purpose is specified in Part 8 of this Ordinance as a purpose in relation to which personal data is exempt from the provisions of data protection principle 6.

(Amended 18 of 2012 s. 40; E.R. 1 of 2013)

2. Principle 2—accuracy and duration of retention of personal data

(1) All practicable steps shall be taken to ensure that—

(a) personal data is accurate having regard to the purpose (including any directly related purpose) for which the personal data is or is to be used;

(b) where there are reasonable grounds for believing that personal data is inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used—
(Amended 18 of 2012 s. 40)

(i) the data is not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise; or

(ii) the data is erased;

(c) where it is practicable in all the circumstances of the case to know that—

(i) personal data disclosed on or after the appointed day to a third party is materially inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used by the third party; and

(ii) that data was inaccurate at the time of such disclosure,

that the third party—

(A) is informed that the data is inaccurate; and

(B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose. *(Amended 18 of 2012 s. 40)*

(2) All practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data is or is to be used. *(Amended 18 of 2012 s. 40)*

(3) Without limiting subsection (2), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data. *(Added 18 of 2012 s. 40)*

(4) In subsection (3)—

data processor (資料處理者) means a person who—

(a) processes personal data on behalf of another person; and

(b) does not process the data for any of the person's own purposes. *(Added 18 of 2012 s. 40)*

3. Principle 3—use of personal data

(1) Personal data shall not, without the prescribed consent of the data subject, be used for a new purpose. *(Amended 18 of 2012 s. 40)*

(2) A relevant person in relation to a data subject may, on his or her behalf, give the prescribed consent required for using his or her personal data for a new purpose if—

(a) the data subject is—

(i) a minor;

(ii) incapable of managing his or her own affairs; or

(iii) mentally incapacitated within the meaning of section 2 of the Mental Health Ordinance (Cap. 136);

(b) the data subject is incapable of understanding the new purpose and deciding whether to give the prescribed consent; and

(c) the relevant person has reasonable grounds for believing that the use of the data for the new purpose is clearly in the interest of the data subject. *(Added 18 of 2012 s. 40)*

(3) A data user must not use the personal data of a data subject for a new purpose even if the prescribed consent for so using that data has been given under subsection (2) by a relevant person, unless the data user has reasonable grounds for believing that the use of that data for the new purpose is clearly in the interest of the data subject. *(Added 18 of 2012 s. 40)*

(4) In this section—

new purpose (新目的), in relation to the use of personal data, means any purpose other than—

(a) the purpose for which the data was to be used at the time of the collection of the data; or

(b) a purpose directly related to the purpose referred to in paragraph (a). *(Added 18 of 2012 s. 40)*

4. Principle 4—security of personal data

(1) All practicable steps shall be taken to ensure that any personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user is protected against unauthorized or accidental access, processing, erasure, loss or use having particular regard to— *(Amended 18 of 2012 s. 40; 17 of 2018 s. 129)*

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data is stored; *(Amended 18 of 2012 s. 40)*

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored; *(Amended 18 of 2012 s. 40)*

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(e) any measures taken for ensuring the secure transmission of the data.

(2) Without limiting subsection (1), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing. *(Added 18 of 2012 s. 40)*

(3) In subsection (2)—

data processor (資料處理者) has the same meaning given by subsection (4) of data protection principle 2. *(Added 18 of 2012 s. 40)*

5. Principle 5—information to be generally available

All practicable steps shall be taken to ensure that a person can—

(a) ascertain a data user's policies and practices in relation to personal data;

(b) be informed of the kind of personal data held by a data user;

(c) be informed of the main purposes for which personal data held by a data user is or is to be used. *(Amended 18 of 2012 s. 40)*

6. Principle 6—access to personal data

A data subject shall be entitled to—

(a) ascertain whether a data user holds personal data of which he is the data subject;

(b) request access to personal data—

(i) within a reasonable time;

(ii) at a fee, if any, that is not excessive;

(iii) in a reasonable manner; and

(iv) in a form that is intelligible;

(c) be given reasons if a request referred to in paragraph (b) is refused;

(d) object to a refusal referred to in paragraph (c);

(e) request the correction of personal data;

(f) be given reasons if a request referred to in paragraph (e) is refused; and

(g) object to a refusal referred to in paragraph (f).

Appendix B

Code of Practice on Consumer Credit Data (extract)

Data Security and System Integrity Safeguards by CRA

Measures to Take in Preparation for Providing Consumer Credit Reference Service

3.11 On or before providing consumer credit reference service to a credit provider, a CRA shall take appropriate measures, including the following, to safeguard against any improper access to or mishandling of consumer credit data held by it:

3.11.1 enter into a formal written agreement with the credit provider as subscriber for such service, which shall specify:

3.11.1.1 the duty of both parties to comply with the Code in providing and in utilising the consumer credit reference service;

3.11.1.2 the conditions under which the credit provider may access consumer credit data held by the CRA; and

3.11.1.3 the controls and procedures to be applied when such credit provider seeks access to the CRA's database;

3.11.2 establish controls to ensure that only data to which a subscriber is entitled is released;

3.11.3 train staff in relation to the Ordinance and the Code and, in particular, good security practice;

3.11.4 develop written guidelines, and disciplinary or contractual procedures in relation to the proper use of access authorities by staff, external contractors or subscribers; and

3.11.5 ensure that adequate protection exists to minimise, as far as possible, the risk of unauthorised entry into the database or interception of communications made to and from the database.

Measures to Take in Daily Operations

3.12 A CRA shall take appropriate measures in its daily operations, including the following, to safeguard against any improper access to or mishandling of consumer credit data held by it:

3.12.1 review on a regular and frequent basis its password controls which help to ensure that only authorised staff are allowed access to its database;

3.12.2 monitor and review on a regular and frequent basis usage of the database, with a view to detecting and investigating any unusual or irregular patterns of access or use;

3.12.3 ensure that practices in relation to the deletion and disposal of data are secure, especially where records or discs are to be disposed of off-site or by external contractors; and

3.12.4 maintain a log of all incidents involving a proven or suspected breach of security, which includes an indication of the records affected, an explanation of the circumstances and action taken.

Log of Access etc. by Credit Provider

3.13 Without prejudice to the generality of clause 3.12 above, a CRA shall:

3.13.1 in the case of there being any suspected abnormal access by a credit provider, report such suspected abnormal access as soon as reasonably practicable to the senior management of the credit provider and to the Commissioner;

3.13.2 maintain a log of all instances of access to its database by credit providers, which log shall include:

3.13.2.1 the identity of the credit provider seeking access;

3.13.2.2 the date and time of access;

3.13.2.3 the identity of the individual whose data was so accessed;

3.13.2.4 the circumstances provided for in clause 2.8, 2.9, 2.9A or 2.10A under which the access has been made (as confirmed by the credit provider pursuant to clause 2.11.1);

3.13.2.5 in the case where the access has been made in the course of the review of existing consumer credit facilities under clause 2.9.1.2, 2.9A.2, 2.9A.4, 2.9A.5, 2.10A.2, 2.10A.3 or 2.10A.4, the specific matter or matters provided for in clause 2.9.3, 2.9.4 or 2.9.5 (as confirmed by the credit provider pursuant to clause 2.11.2); and

3.13.2.6 instances of reporting by the CRA of suspected abnormal access to the senior management of a credit provider and to the Commissioner,

and shall keep such a log for not less than 2 years for examination by its compliance auditor and/or by the Commissioner, as the case may be.