Cold Storage Singapore (1983) Pte Ltd
Co. Reg. No. 194700005R
21 Tampines North Drive 2 #03-01 Singapore 528765
Tel: (65) 6891 8000

COLD STORAGE SINGAPORE (1983) PTE LTD

RESPONSE TO THE PUBLIC CONSULTATION PAPER ("PCP") ON THE DRAFT PERSONAL DATA PROTECTION (AMENDMENT) BILL ("AMENDMENT BILL") DATED 14/05/2020

28 May 2020

(A) GENERAL INTRODUCTION OF COLD STORAGE SINGAPORE (1983) PTE LTD ("CSS")

1. CSS is one of the food retailers incorporated in Singapore, managing and operating chain of supermarkets, convenience stores and health and beauty outlets under the well-known brands of Cold Storage, Giant, 7-Eleven and Guardian.

2. CSS is grateful for this opportunity to provide our feedbacks and inputs in respect of the Personal Date Protection (Amendments) Bill.

(B) SUMMARY OF MAJOR POINTS

1. CSS welcomes the "deemed consent by notification" and the "business improvement purpose" as it would be helpful for businesses to improve and enhance our interactions with and products/services provided to our customers.

2. CSS also fully supports on the accountability-based approach in respect of the mandatory data breach notification. However, we wish PDPC could consider introducing some forms of exceptions / defences to organisations as mentioned in our comments below.

3. CSS also urges PDPC to re-consider on the increased monetary fines based on our justifications mentioned in our comments below.

(C) COMMENTS

1. Accountability Principle

We have no comment on Paragraphs 10 to 12 of the PCP.

2. Mandatory Data Breach Notification Requirement

2.1 Notification criteria:

2.1.1 With respect to the notification criteria under Paragraphs 16, 17 and 18 of the PCP that Organisations will be required to notify PDPC of a data breach that (i) results in, or is likely to result, in **significant harm** to the individuals to whom any personal data affected by a data breach relates (the "affected individuals"); or (ii) is of a **significant scale**.

2.1.2 We have no comment on the threshold of significant scale being "500 or more affected individuals" stated in Paragraph 17.

2.1.3 Referring to the prescribed category of personal data which may probably include credit and debit card numbers, if the retailer's point-of-sale does not collect full 16-digit credit/debit card numbers, would any leakage of such data (first 4 and last 4 digit or partial credit/debit card numbers currently collected by the retailer) be considered of satisfying the notification criteria under proposed Sec 26B(2) of the Amendment Bill?

2.1.4 Similarly, partial NRIC numbers or any identification numbers currently collected by organisations are still treated as "personal data" under the PDPA. Would any data breach in respect of partial identification numbers trigger this notification requirement?

2.1.5 Please also see our comments in Paragraph 2.3.1 below.

2.2 Assessment and Notification Timeframe:

2.2.1 We suggest PDPC to consider the notification timeframe of "3 working days" instead of "3 calendar days", if a data breach meets the criteria for notifying PDPC, after the day the organisation determines that the data breach meets the notification criteria.

2.2.2 Meanwhile, in respect of the data intermediary's ("DI") duty to notify the organisation "without undue delay" when it has reason to believe that a data breach has occurred in relation to personal data that the data intermediary is processing on behalf of and for the purposes of another organisation under proposed Sec 26D(2) of the Amendment Bill, would PDPC define and cap the "without undue delay" within 24 hours as currently required under the Guide to Managing Data Breach 2.0?

2.3 Exceptions to the Notification Requirement (to affected individual):

2.3.1 We welcome the exceptions (remedial action and technological protection exceptions) set out in Paragraph 22 of the PCP and Sec 26D(4) and (5) of the Amendment Bill. However, would PDPC consider including "partial data" i.e. partial credit/debit card numbers or partial identification numbers as an exception to the notification requirement?

2.3.2 We noted that organisations are not required to notify (under the proposed Sec 26D(6)(b) of the Amendment Bill) the affected individual if the PDPC so directs. As such, would PDPC prescribe a timeline for organisations to notify the affected individual given that organisation may notify both the PDPC and the affected individual simultaneously. Further, would PDPC be able to provide immediate advice or direction to organisation to not notify any affected individual?

3. Removal Of Exclusions For Organisations Acting On Behalf Of Public Agencies

We have no comment on Paragraphs 27 to 29 of the PCP.

4. Offences Relating To Egregious Mishandling Of Personal Data

4.1 We welcome the strengthened accountability of individual employee by introducing offences to such individual for egregious mishandling of personal data in the possession of or under the control of an organisation.

4.2 We also noted PDPC's policy position stated in Paragraph 31 of the PCP that the PDPC may hold organisations primarily accountable for breach of data protection due to the actions/misconducts of their employees in the course of their employment with the organisations.

4.3 In many cases, the affected organisation may not be aware of or involved in the "misconduct" carried out by the employee (e.g. improper use of customers' personal data for personal gain) until and unless it is reported by an affected customer. If the affected organisation is to be punished by the PDPC for the misconduct/breach by reporting such misconduct or misbehaviour of its employee to the PDPC, this may possibly deter an organisation from reporting such misconduct or mishandling to the PDPC. This would go against PDPC's will to strengthen personal/individual's accountability.

4.4 Hence, would PDPC consider offering some form of protection/defence/immunity under the Amendment Bill to such affected organisation who honestly report a misconduct/mishandling of personal data to the PDPC or who have in place the appropriate measures but was still subject to personal actions/misconducts of their employees in the course of their employment with the organisations?

5. Enhanced Framework For Collection, Use and Disclosure Of Personal Data

5.1 We have no comment on the "deemed consent by contractual necessity" and the "legitimate interest exception" as stated in Paragraphs 38(a) and 40(a) of the PCP.

5.2 Meanwhile, referring to the "deemed consent by notification", we noted that this "deemed consent by notification" shall not apply to direct marketing messages. It is important for retailers to reach out to their customers by sending marketing messages promoting the retailers' products for more business opportunities. As long as the customers/consumers

are given reasonable time and manner to opt-out, we urge PDPC to consider allowing the same.

5.3 Meanwhile, for new "Business Improvement Exception" under Paragraph 40(b) of the PCP which allows organisations to use personal data without consent for business improvement purposes. Please clarify whether the use by organisations under Part 2 of the proposed Second Schedule of the Amendment Bill covers disclosure of customers' personal data by the organisation to its third-party service provider (e.g. consultant for customer relation and business insight/analytic) which may use such personal data for the improvement of the organisation's business.

6. Data Portability Obligations

We have no comment on Paragraphs 43 to 52 of the PCP.

7. Improved Controls For Unsolicited Commercial Messages; Enforcement Of DNC Provisions Under Administrative Regime

We have no comment on Paragraphs 53 to 57 of the PCP.

8. Increased Financial Penalty Cap

8.1 We noted that the maximum financial penalty will be increased to (i) 10% of the organisation's annual gross turnover in Singapore (for organisation with an annual turnover exceeding S$10 million); or (ii) S$1 million, whichever is higher.

8.2 We understand the PDPC's intention of having a stronger deterrent, but the 10% annual gross turnover may be exorbitant for organisations which do not process or use personal data for trade (e.g. cloud service providers, data analytics firms, etc.) as their core business activities. We suggest PDPC to consider setting some clarities on imposing any fine which is more than S$1 million, e.g. such data breach is of a significant scale or causes significant harm to the affected individuals or setting different tiers of penalty amount on organisations based on the nature of their core businesses.

9. Require Attendance; Statutory Undertakings

We have no comment on Paragraphs 61 to 67 of the PCP.

10. Referral To Mediation

10.1 We noted that the PDPC may refer the disputes between the complainant and organisation to a mediation without the consents of the complainant and the organisation. The proposed Sec 27(4) of the Amendment Bill empowers the PDPC to make regulations for matters relating to the operation of an operator of a mediation scheme, inter alia, the fees that the operator may charge.

10.2 We would like to seek clarifications from PDPC on whether:

(a) either the complainant or the organisation, or both parties could opt out from the mediation scheme despite the referral by the PDPC?

(b) would the PDPC consider the principle of costs follow the event that the unsuccessful party ruled against by the mediator/operator to bear all costs including the fees of the operator?

11. Preservation Of Personal data requested pursuant to access and porting requests

11.1 We refer to the prescribed period mentioned in Paragraph 72 of the PCP:

(a) The prescribed 30 calendar days' period after the rejection of access request is reasonable for organisation's compliance.

(b) However, the second limb *"until the individual has exhausted his/her right to apply for a reconsideration request to PDPC or appeal to the Data Protection Appeal Committee, High Court or Court of Appeal, whichever is later"* poses uncertainty on the organisation whether to keep such personal data after the prescribed 30 days' period without any clear indication/notification from the customer/individual that he or she will take further actions for such access request.

11.2 Hence, it would be helpful if the PDPC could set some criteria that the second limb would apply, e.g. the organisation is served by written notification that the customer/individual has filed such appeal or application to the relevant authority within the prescribed 30 days' period.

12. Prohibitions To Providing Access

12.1 We noted that an organisation is allowed to provide access to personal data to the requester (let's call him "Requester A") even though such data may reveal the personal data or identity of another person (let's call him/her "Party B") that does not consent to such disclosure of his/her personal data to the Requester A.

12.2 If the same Party B, at some later time, makes a request to access to his/her personal data under Sec 21(1) of the PDPA, an organisation is required under Sec 21(1)(b) to provide information about the ways in which his/her personal data referred to in Sec 21(1)(a) has been or may have been used or disclosed by the organisation within a year before the date of the Party B's request including the fact that the organisation has disclosed Party B's personal data to the Requester A which happened within the prescribed one-year time period.

12.3 Given the difficulty of tracing the identities of each individual (especially for CCTV footage that captures numerous individuals), would the PDPC consider expanding the scope of the proposed Sec 21(4) that the organisation is not required to inform an individual under Sec 21(1)(b) if the disclosure is made pursuant to the proposed Sec 21(3A) of the Amendment Bill?

13. Excluding "derived personal data" From Correction And Data Portability Obligations

We have no comment on Paragraphs 76 and 77 of the PCP.

14. Revised Exceptions To Consent Obligation

Please refer to our comments in Paragraph 5.2 above in respect of the proposed Sec 17(1)(b) and Sec 17(2)(b) of the Amendment Bill that the organisation should be allowed not only to use but to disclose such personal data to its third-party consultant for purpose of improvement of the organisation's business (e.g. customer relations/business analytic services).

(D) CONCLUSION

We appreciate your considerations on our feedback mentioned above, and you may contact us at the following email address should you need further clarifications or additional information.

Lee Mun Yee
Legal Counsel
Mobile: 98595139
Email: muylee@coldstorage.com.sg