**Annex**

## Guidance on Sharing Customer Data by Authorized Institutions for Direct Marketing by Third Parties

While authorized institutions ("AIs") collect personal data of customers through online channels including mobile apps for their own operational and direct marketing [1] purposes, there are increasing occasions where AIs may also provide such personal data collected to third parties such that the third parties may use such personal data for their own direct marketing purpose. In order to better safeguard personal data of banking customers, AIs should observe the following guidance principles.

### 1. Scope of the guidance

1.1 This guidance is applicable to provision of customers' personal data by AIs to third parties, including group companies of AIs (collectively referred to as "third parties"), for the purpose of usage by the third parties for direct marketing. There should not be distinction in collection or provision of customers' personal data between different processes of banking products or services, such as during or subsequent to account opening and application process for banking products or services; nor distinction between different business lines (e.g. retail banking or commercial banking, etc.).

1.2 Since this guidance focuses on sharing of customers' personal data for direct marketing by third parties, the sharing of customers' personal data to third parties in the following situations will generally not be subject to this guidance:

(i) the sharing of customers' personal data is for the purpose of carrying out AI's own functions or activities, e.g. servicing of products jointly administered by the AI and a third party, or administered by a third party on behalf of the AI under an outsourcing arrangement;

(ii) the AI is acting on behalf of the customer, such as in many applicable settings in respect of private banking business that do not involve directing marketing by third parties;

(iii) the arrangements fall under the Open Application Programming Interface ("API") Framework, where they are subject to a separate set of applicable requirements; and

(iv) the arrangements fall under specific initiatives to facilitate and strengthen the convenient flow of people, goods and funds in the Guangdong-Hong Kong-Macao Greater Bay Area ("GBA"), such as the Cross-boundary Wealth Management Connect scheme ("Cross-boundary WMC"), where they are subject to separate sets of applicable requirements.

---

[1] As defined in section 35A of Part 6A to the Personal Data (Privacy) Ordinance ("PDPO"). Reference can also be made to New Guidance on Direct Marketing issued by Privacy Commissioner for Personal Data, Hong Kong ("PCPD").

## 2. Approaches for sharing customers' personal data

AIs may adopt either of the following approaches for sharing customers' personal data collected through online channels (including mobile apps)[2] to third parties for the purpose of direct marketing by the third parties:

Approach A: ask customers to directly approach the third parties; or

Approach B: redirect customers to the third parties.

### *2.1 Approach A: Ask customers to directly approach the third parties*

Instead of AIs passing customers' personal data to third parties, it would be clearer to the customers if they provide their personal data directly to the third parties. Under this approach, AIs do not share customers' personal data to third parties, but ask customers to directly visit the websites / mobile apps of the third parties where the customers can (i) input their personal data and/or (ii) provide their consent directly to the third parties for the purpose of direct marketing by the third parties.

### *2.2 Approach B: Redirect customers to the third parties*

Under this approach, AIs may redirect customers from AIs' website / mobile apps to the websites / mobile apps of the third parties ("redirection") where customers can (i) input their personal data and/or (ii) provide their consent directly to the third parties for the purpose of direct marketing by the third parties.

(a) AIs are required to perform the redirection in a proper manner as follows:

(i) AIs should provide customers with reminder message **before** the redirection is performed that customers will be redirected from AIs to the third parties;

(ii) AIs should explain to customers in the reminder message the purpose(s) of such redirection;

(iii) Reminder messages and disclosure of the purpose(s) of redirection should be clear, explicit, straightforward, in a reasonable layout and font size that is readily readable, and understandable; and

(iv) AIs should not bundle the redirection and/or any transfer of personal data of customers to third parties in the process of bank account opening or provision of banking services. There may be circumstances where AIs may have collaboration with third parties in promotional activities of banking services which may require customers' sharing of personal data in order to enjoy the promotional offers. In such cases, the process of account opening or provision of basic banking services should not be adversely affected for the reason of refusal of sharing of personal data by a customer to a third party.

---

[2] Refer to channels where financial services of AIs are delivered over the Internet to customers' devices including personal computers and mobile devices.

## 3. Sharing of customers' personal data

### *3.1 Types of customers' personal data that may be shared with third parties under "redirection"*

(a) In case there are any circumstances (e.g. registration of promotional programmes, getting promotional offers provided by third parties, etc.) that AIs have the need to provide personal data of customers to third parties under Approach B (i.e. redirection mentioned in paragraph 2) AIs should pay attention to the Data Protection Principle 1 under the PDPO that the data collected should be necessary and adequate but not excessive.

(b) AIs should pay due regard to the principle of "data minimisation", i.e. the shareable scope of data should be what the data recipient actually needs under the circumstances. Excessive and irrelevant personal data of customers should not be shared. AIs should (i) carefully assess what kinds of data the data recipients would require, and (ii) only share minimum customers' personal data on a "need-to-know" basis.

(c) Explicit consent of customers for sharing the customers' personal data to third parties should be obtained before the redirection. Such customer consent is only for sharing customers' personal data to the third parties under paragraph 2.2(a), and should not cover obtaining customer's consent for direct marketing by the third parties. AIs should also, among others, make reference to the relevant requirements under sections 35J and 35K of the PDPO. For the avoidance of doubt, if there is no customers' personal data shared with third parties, no such customer consent is required, but AIs should still provide customers with a reminder message about redirection as mentioned in paragraph 2.2(a).

(d) In addition, the types of customer personal data to be shared by AIs are further confined depending on the nature of third parties:

(i) To third parties which are regulated by the Hong Kong Monetary Authority, Insurance Authority, Mandatory Provident Fund Schemes Authority or Securities and Futures Commission, as well as those third parties which are licensed to operate a banking business or a business of taking deposits in a place outside Hong Kong and regulated by a supervisory authority there: AIs may, at most, share customers' names, email addresses and/or mobile numbers.

(ii) To third parties other than (i): AIs may, at most, share customers' email addresses.

### *3.2 Sharing of personal data of individuals other than the customers themselves*

It is not appropriate for AIs to seek and rely on their own customers' consent to obtain personal data of any other individuals (e.g. contact information of relatives

or friends of a retail bank customer, or staff of a corporate customer), whether these individuals are bank customers or not (i.e. without seeking consent directly from those individuals). It follows that, personal data of such individuals should not be shared with third parties (e.g. referral agents, collaboration partners of banking events or promotional programmes, etc.) for the purpose of direct marketing by the third parties.

## 4. Other guiding principles on sharing customers' personal data to third parties

AIs which share customers' personal data to third parties are also reminded to follow the key guiding principles below where applicable:

4.1 Any transfer of customers' personal data to third parties must be in strict compliance with all the relevant requirements of PDPO and relevant codes of practice issued or approved by the PCPD giving practical guidance on compliance with the PDPO.

### *4.2 Data Security*

(a) Data Protection Principle 4 under the PDPO requires that data users take all practicable steps to protect the personal data they hold against unauthorised or accidental access, processing, erasure, loss or use.

(b) AIs should take reasonably practicable steps to safeguard the security of shared data during transit of customers' personal data to third parties.

(c) AIs are reminded the importance of data security and required to put in place some practicable security measures, for example, by encryption of personal data during data sharing process.

### *4.3 Data Ethics*

(a) AIs are encouraged to consider the three core values of data ethics, namely Respectful, Beneficial and Fair, when handling customer data, including the following general principles:
   (i) accountability for sharing of customers' personal data to third parties for direct marketing;
   (ii) the sharing of customers' personal data being explainable and reasonable;
   (iii) implementing measures to mitigate all the identified risks and balance the interests of customers, not just taking into account the benefits of the AIs and third parties alone;
   (iv) conducting a privacy impact assessment ("PIA") before the commencement of the collaboration programmes with third parties, to assess the risks and benefits of data sharing. AIs may refer to the information related to PIA issued by PDPO;
   (v) the sharing of customers' personal data to third parties being fair with no unequal treatment or discrimination; and

(vi) all the process related to sharing with third parties of customers' personal data for direct marketing being properly documented.

(b) AIs are also encouraged to develop a culture of ethical data governance which should, among others, well define the accountability of the relevant departments and staff of the AIs in handling customers' personal data.

### *4.4 Treat Customers Fairly*

(a) AIs are reminded to treat all customers equitably, honestly and fairly at all stages of provision of banking products or services which involve sharing of customers' personal data to third parties.

(b) Where customers' personal data sharing with third parties is not a one-off exercise, AIs should, among others, clearly inform and remind customers the following where applicable:

(i) Customers have the right to refuse to give the consent or withdraw the consent given to AIs for sharing their personal information to third parties if they so request. When a customer objects to the disclosure of the information he/she provided to AIs or refuses to give the consent or withdraws any consent given to AIs for sharing his/her personal information to third parties, AIs should give effect to such objection, refusal or withdrawal and should not refuse to provide that customer with the relevant banking services.

(ii) Customers should be reminded at least once every year or by including a standard notice in their marketing materials of relevant banking services of the right to make the request referred to in the above.

### *4.5 Monitoring and Control*

(a) AIs should keep proper track of the customers' personal data shared to third parties for the purpose of direct marketing by the third parties.

(b) AIs are required to put in place proper monitoring and control measures with sufficient management oversight regarding the AIs' compliance with all the applicable regulatory requirements as well as AIs' policies and procedures related to customer data protection. AIs are also required to conduct regular independent reviews (e.g. by internal audit) on the effectiveness of the monitoring and control measures.

### *4.6 Data Sharing Agreement*

(a) AIs may consider entering into a data sharing agreement ("DSA") with third parties, which effectively setting out proper terms and conditions (as well as the rights and obligations) for the sharing of customer data between AIs and third parties.

(b) A DSA helps protecting the rights and interests of customers who provide data to AIs. In the event of data breach and/or customer data leakage incident, a clear DSA can also assist the data provider and data recipient in distinguishing their obligations and liabilities.