Tips for Using Fintech

PCPD HK

PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

To protect personal data privacy, consumers should adopt the following measures in the use of Fintech:

1. Carefully read the privacy policies, particularly :

- the types of personal data to be collected
- the possible use of the personal data
- the potential transferees of the personal data
- consumers' rights and obligations with respect to their personal data, such as rights to access, rectify and opt out of certain uses
- security measures adopted by the organisations to protect personal data

2. Critically assess requests for personal data, review privacy settings and remove unnecessary access rights of the Fintech application softwares

3. Operate Fintech application softwares under a safe environment:

- do not operate the application softwares via public or insecure Wi-Fi, or on public computers
- ensure anti-theft features have been switched on and the latest security patch and anti-virus softwares have been installed on the device on which the application softwares operate
- use complex passwords for the accounts, and do not share the passwords with other accounts

4. Monitor accounts regularly to spot unauthorised transactions/activities

Recommended **Good Practices** for **Fintech** Providers/Operators

1. **The privacy policies should be transparent and written in plain and user-friendly languages to explain the following:**
   - the types of personal data to be collected and its necessity
   - all intended uses of the personal data
   - all possible transferees of the personal data
   - consumers' rights and obligations, such as rights to access, rectify and opt out of certain uses
   - the security measures adopted for personal data protection

2. **Collect and retain minimum amount of personal data**

3. **Provide clear and genuine options to consumers with respect to collection and use of personal data**
   - Clear option: prominently brought to the consumers' attention, rather than buried in the lengthy privacy policies
   - Genuine option: consumers' choices will not have significant adverse impact on their access to, and the costs and benefits of the services

4. **Ensure the accuracy and impartiality of the personal data**

5. **Ensure the reliability and fairness of Fintech algorithms, and provide consumers with explanations on the automatic assessments and decisions (e.g. credit score) by the Fintech**

6. **Adopt appropriate policies, procedures and techniques to safeguard personal data**

7. **Adopt contractual or other means (e.g. field audit) to ensure proper protection to personal data by data processors**

8. **Conduct Privacy Impact Assessment at or before the development stage of Fintech so as to identify and properly address potential privacy risks**

9. **Adopt privacy-friendly design in Fintech**

10. **Develop procedures in relation to handling of data breach incidents**

Download
this publication

Enquiry Hotline	**:**	**(852) 2827 2827**
Fax	**:**	**(852) 2877 7026**
Address	**:**	**Room 1303, 13/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong**
Email	**:**	**enquiry@pcpd.org.hk**

Copyright

Disclaimer

The information and suggestions provided in this publication are for general reference only. They do not serve as an exhaustive guide to the application of the law. The Privacy Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided will not affect the functions and powers conferred upon the Privacy Commissioner under the Personal Data (Privacy) Ordinance.

First published in March 2019

PCPD
H K
PCPD.org.hk

Information Leaflet

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Fintech

1. Introduction

1.1 Fintech, being the short form of "financial technology", refers to the information and communication technology used for the provision of financial services. Fintech may involve different types of technologies and may come in different forms. It enables innovation in financial services, and is transforming the operations of the financial industry. Fintech is also penetrating into many aspects of our daily lives.

1.2 This publication aims to:

(a) introduce some common applications of Fintech with privacy implications;

(b) explain the privacy risk of the Fintech applications;

(c) provide tips to consumers/users for protecting their personal data privacy when using Fintech; and

(d) recommend good practices to providers/operators of Fintech for addressing the privacy risks of Fintech.

1.3 There may be other non-privacy related risks associated with the use of Fintech (such as financial risks) which are outside the remit of the Personal Data (Privacy) Ordinance, (Chapter 486 of the Laws of Hong Kong) (**Ordinance**) and the Privacy Commissioner for Personal Data (**Privacy Commissioner**). Non-privacy related risks are beyond the scope of this Information Leaflet. Providers/operators of Fintech should check whether they are subject to other industry-specific regulations.

2. Common Applications of Fintech

2.1 There is no precise boundary of Fintech. The advancement in computational powers, Internet connectivity and mobile technologies, together with the strong demand for efficient, low-cost and personalised financial services, have given a strong boost to the proliferation of Fintech.

2.2 Fintech may come in different forms, and support different kinds of financial services and operations, such as:

(a) electronic payments and remittances (e.g. e-wallet[1]);

(b) financial investments (e.g. robo-advisors and algorithmic trading);

(c) peer-to-peer (**P2P**) financing (e.g. P2P lending and crowdfunding);

(d) data analytics that support the operations of financial institutions (e.g. credit scoring);

(e) information sharing (e.g. open Application Programme Interface (**API**); and

(f) Distributed Ledger Technology (**DLT**) (a specific type of DLT is blockchain technology; examples of uses of DLT include cryptocurrency transactions and smart contract applications).

2.3 Not all Fintech involves the collection and processing of personal data. Even if it does, the level of risks to personal data privacy posed will vary by the Fintech in question, depending on the volume, sensitivity and intended use of personal data, and the data governance of the providers/operators

[1] E-wallets include Stored Value Facilities (SVFs) regulated under the Payment Systems and Stored Value Facilities Ordinance (Chapter 584 of the Laws of Hong Kong). However, not all e-wallets belong to SVFs, particularly for those without store-value function.

of Fintech, among other things. Below are some common examples of Fintech which may well involve collection and/or processing of personal data, and hence giving rise to privacy risks.

Electronic payment

2.4 Electronic payments are payments made through application software (usually operating in a mobile phone). Electronic payments allow users to pay electronically at brick-and-mortar stores or online shops, or make P2P transfers of money. An electronic payment may be made by scanning a QR code, tapping a mobile phone on a merchant's contactless reader, or keying in payment details in a mobile application.

2.5 A provider of electronic payment service may collect users' personal data at different stages. For example, a user is usually required to provide his or her name, email address, mobile phone number and bank account information to the service provider during the registration stage. Some service providers may also require users to provide identity proof (e.g. a copy of Hong Kong Identity Card) for completing the know-your-customer process as prescribed by the financial regulations. During the operation stage, a service provider will record the payment details, such as date, time, monetary value and location of a payment. The relevant software application of electronic payment service may also require access to the user's phone book in a mobile phone for processing P2P payments.

Credit scoring

2.6 Credit scoring refers to a method of assessing a person's creditworthiness using mathematical models. Traditionally, a lender uses information such as an individual's banking transactions history, credit history and income proof for conducting the assessment. With the advancement in the technology of data analytics, big data analytics and scoring algorithms, it may now be used to analyse different kinds of personal data of a borrower to determine his or her credit score. The personal data that may be used in the assessment includes purchase history, payment records, neighbourhood, social network and other behavioural data.

Open API

2.7 An API is a tool that enables different application softwares, both within an organisation and among organisations, to interact and communicate. An API can facilitate efficient and secure transmission of data among application softwares. Open API is an API that provides third-party programme developers with access to another organisation's data with minimum restrictions. The third-party developers may then make use of the data to create new services to consumers.

2.8 In the context of Fintech, an open API may involve the sharing of customers' account information (e.g. balances or transactions) by banks with third-party programme developers, under the authorisation of the customers concerned[2]. A developer may then create an application software that allows users to manage their accounts in different banks in one single platform, and in real time. A lender may also make use of the reliable data from the open APIs of banks to assess the creditworthiness of its prospective borrowers. An open API may also involve the sharing of non-personal data, such as interest rates and service charges of banks.

DLT and Blockchain

2.9 DLT is a digital ledger that allows transactions and data to be recorded, shared, and synchronised across a distributed network of different network participants. Blockchain is a specific type of DLT, and is gaining impetus.

2.10 In a blockchain, data is stored and transmitted in packages called "blocks", which are connected to one another by a digital "chain". A new block is created when a valid transaction is made. The digital chain, in reality, is made up of the cryptographic hashes of the blocks. Each block in a blockchain contains the cryptographic hash of its previous block so that the blocks are connected to one another to form a chain. The cryptographic hashes help confirming the integrity of the blocks, as well as tracing any single block all the way back to the original genesis block.

2.11 A blockchain is a distributed ledger because each participant of it has an identical copy of the whole ledger, i.e. the whole blockchain. Cryptographic and algorithmic methods are employed to record and synchronise data across the entire network.

2.12 Each new transaction in a blockchain has to be validated by the network participants. The resulting block is then linked to the existing chain of blocks. As new blocks are added, the linear chain grows. Earlier blocks cannot be retrospectively altered or deleted by any network participant. Therefore, a blockchain is intended to be immutable.

[2] Reference: "*Open API Framework for the Hong Kong Banking Sector*" published by the Hong Kong Monetary Authority on 18 July 2018: https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2018/20180718e5a2.pdf

2.13 A blockchain, if designed and built properly, is said to be tamper-proof under the current technology level. It is also said to guarantee trust among participants as to the integrity of records. A blockchain is generally highly transparent because all transactions are public, traceable and permanently stored in the blocks.

2.14 Currently, the most well-known use of blockchain is for recording transactions of cryptocurrencies, such as Bitcoins. Blockchains, or DLT, may also be used for many other financial operations, such as international payment and remittance, payment authorisation, clearance and settlement, trading of securities and notarisation service for mortgages. Other non-financial uses of DLT and blockchain may include supply chain management, rewards and loyalty programme.

3. Privacy Risks of Fintech

3.1 While Fintech may provide many benefits to both the operators and customers, there are privacy risks associated with the use of Fintech.

Collection and use of personal data without notice or meaningful consent of the users

3.2 A host of personal data may be collected or generated with the use of Fintech, with or without a user's notice[3]. The personal data may then be used or disclosed by the providers/operators of Fintech beyond the users' reasonable expectations, or without the users' meaningful consent[4].

Electronic Payment

3.3 In addition to mobile phone number and identity proof knowingly provided by users during registration, an electronic payment service provider may also collect the contact lists, purchase histories and location data of the users, with or without the users' notice. The personal data collected may enable the service provider to weave various aspects of the users' lives together like mosaic and accurately predict their behaviours, preferences and habits by profiling. Sometimes the profiling may reveal sensitive personal data or personal secrets of the users. The collected and inferred personal data may then be used in, for example, personalised advertisements and credit scoring without the users' notice or meaningful consent.

Credit scoring

3.4 Credit scoring involves the use of big data analytics and scoring algorithms for assessing individuals' financial standing. The sources of data are diverse. It may include individuals' purchasing patterns, timeliness of bill payments, posts on social media and other information. The data used and inputted for analysis may be beyond the individuals' reasonable expectations. Low transparency may also render individuals unable to control the use of their personal data and protect themselves, such as challenging an inappropriate decision based on inaccurate or biased personal data of theirs. If individuals are kept in the dark regarding the use of their personal data in generating a credit score, they may experience an affront to respect and dignity when the facts come to light.

Open API

3.5 In an open API, an individual may not have full understanding on the kinds of personal data that is shared with third-party developers, and how the personal data may be used and further disclosed. This is particularly the case when the restriction to access the open API is low, and the privacy and data security policies and practices of the third-party developers are unclear.

Blockchain

3.6 In a blockchain, new participants may be admitted to the network from time to time, and each participant will have a copy of the whole digital ledger. Existing participants may have no idea about who else will have access to their records in future. This problem is particularly acute for "permissionless blockchains", which are public networks that allow anybody to join, read the contents and conduct transactions. In contrast, in private blockchain networks, only authorised parties can join, and the privacy risk is relatively lower.

[3] Data Protection Principle (**DPP**) 1(3) in Schedule 1 to the Ordinance provides that all practicable steps must be taken by a data user to ensure that the data subjects are informed, on or before collection of their personal data, the purpose for which the personal data is to be used and the potential transferees of the personal data, among others.

[4] DPP 3 in Schedule 1 to the Ordinance provides that a data user must obtain express and voluntary consent of the data subjects before using their personal data for new purposes. A "new purpose" is any purpose that is different from or unrelated to the original purpose of collection of the personal data.

Use of personal data in unfair or discriminatory ways

Credit scoring

3.7 Credit scoring algorithms, like many other applications of big data analytics, make assessment on individuals' creditworthiness by mixing and analysing sheer volume of public, private and personal data collected from multiple sources. Personal data of some kinds is collected directly from individuals (e.g. contact information). Personal data of some other kinds may be generated during the interaction between the individual and the lender (e.g. transaction records) or may be inferred by data analytics (e.g. whether an individual is a shopaholic). Therefore, individuals may not be able to obtain a complete picture of the data collected or used for the credit assessment, not to mention verifying the accuracy and relevance of the data[5]. The relationship between some kinds of personal data (e.g. social network and neighbourhood of an individual) and the creditworthiness of an individual may also be dubious. As a result, there is a risk that the data inputted into the assessment is inaccurate, biased, irrelevant or outdated. In the circumstances, the credit scores of the individuals concerned, as well as the individuals' access to credit facilities, may well be unfairly and adversely affected.

Lack of effective means to erase or rectify obsolete or inaccurate personal data

Blockchain

3.8 Blockchains are immutable and tamper proof by design. A "block" cannot be deleted or amended even if the data stored in it is obsolete or inaccurate. The retention and continuous availability of inaccurate or obsolete personal data may well prejudice an individual's rights to personal data privacy[6].

Electronic payment, credit scoring, open API,etc.

3.9 In view of the increasing value of data in the digital economy, service providers/operators of Fintech may be inclined to collect and retain as much personal data as possible, even if the data may be inaccurate, irrelevant or obsolete. They may not have put in place an effective mechanism to erase or rectify the inaccurate, irrelevant or obsolete data in a timely manner. Such practice does not only prejudice individuals' rights to personal data privacy, but increases the risk and impact of data breach, and may be contrary to the law[7].

Data security risks

3.10 Collection and/or processing of personal data will inevitably give rise to data security risk[8]. For example, electronic payments and open APIs involve transmitting personal data electronically among different organisations and end-users, which increases the risk of data leakage or interception during transmission. The wealth of personal data and financial information stored in the databases of Fintech providers/operators may well be treasure troves for hackers. This is particularly the case in the digital era where the value of data is high, thereby increasing the incentive for misappropriation of data. Leakage of personal data may render individuals susceptible to impersonation, scams, harassments, identity thefts and other crimes.

Obscurity of the identities of data users[9] and data processors[10]

3.11 During the use and operation of Fintech, a number of parties may be involved in the processing and storage of personal data. For example, data collected by a Fintech operator may be stored by its cloud service provider and then analysed by a third-party data analytics company. For an open API, a large number of developers may have access to the same individuals' personal data. For a blockchain, the decentralised nature of the digital ledger means that there may not be any central administrator or authority to take responsibility for operation of the network or the

[5] DPP 2(1) in Schedule 1 to the Ordinance provides that all practicable steps must be taken by a data user to ensure that the personal data is accurate having regard to the purpose for which the personal data is or is to be used. The data user must stop using or erase the personal data if there are reasonable grounds for believing that the personal data is inaccurate.

[6] Section 26 and DPP 2(2) of the Ordinance provide that all practicable steps must be taken by a data user to ensure that the personal data is not kept longer than is necessary for the fulfillment of the purpose of collection (including any directly related purpose). Section 22 and DPP 6(e) of the Ordinance provide individuals with the right to correct their personal data that is inaccurate.

[7] Relevant provisions under the Ordinance:
- section 26 and DPP 2(2) regarding retention of personal data; and
- section 22 and DPP 6(e) regarding correction of personal data. (See footnote 6 above.)

[8] DPP 4 in Schedule 1 to the Ordinance provides that all practicable steps must be taken by a data user to ensure that the personal data in its possession is protected against unauthorised or accidental access, processing, erasure, loss or use.

[9] Section 2(1) of the Ordinance defines "data user" as a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of personal data.

[10] DPP 2(4) in Schedule 1 to the Ordinance defines "data processor" as a person who process personal data on behalf of another person, and does not process the data for any of the person's own purposes.

behaviour of the participants. These risks may lead to obscurity as to the identity of the data users and data processors who are responsible for the governance and protection of the personal data[11]. As a result, individuals may not be able to ascertain who is liable for the leakage or mishandling of their personal data.

4. Tips for Users of Fintech

4.1 For the purpose of this publication, a user of Fintech is a consumer who uses Fintech for personal purposes. The tips below aim to assist a user in protecting his/her personal data privacy in the use of Fintech, but are not meant to be exhaustive.

Carefully read the privacy policies

4.2 Whenever personal data is to be collected by a Fintech, privacy policy should be provided by the operator. Users should read the privacy policy carefully to understand their rights and obligations. In particular, users should pay attention to the following:

(a) the types of personal data to be collected by the operator;

(b) the possible use of the personal data by the operator;

(c) the potential transferees of the personal data;

(d) the users' rights (e.g. a right to access and rectify, and a right to opt out of certain uses) and obligations with respect to their personal data; and

(e) the security measures that the operator will adopt to protect the personal data in transit and storage.

Critically assess requests for personal data and review privacy settings

4.3 Depending on their functions, different types of Fintech may require different types of personal data for proper functioning. For example, a provider of electronic payment service and credit assessor may need a user's identity proof for complying with anti-money laundering regulations. However, they may not need to have access to the geolocation data and phone book in the user's mobile phone. Therefore, users should critically assess the functions of Fintech, the types of personal data sought and the purposes, and then decide whether or not to provide the data or proceed with using the services.

4.4 Users should also review the privacy settings of the application softwares of the Fintech, and remove the unnecessary access rights of the application softwares.

Operate the application software of Fintech under a safe environment

4.5 Sensitive personal data such as bank account information and passwords may be processed and transmitted during the use of Fintech. Therefore, application softwares of Fintech, such as electronic payment applications, should only be operated under a safe environment, e.g.:

(a) do not operate the application software of Fintech over public or insecure Wi-Fi connection;

(b) do not operate the application software of Fintech on public computers;

(c) make sure the device on which the application software operates has the appropriate anti-theft features switched on (e.g. screen lock, find-my-phone and remote erasure), and the latest security patch and anti-virus software installed; and

(d) use complex passwords for user accounts, and do not use the same passwords for other less-sensitive services such as social networks.

Monitor account activities regularly

4.6 Users should regularly monitor transaction records or account activities to spot unauthorised transactions/activities, and report the unauthorised transactions/activities to the providers/operators of Fintech as soon as possible.

5. Recommended Good Practices for Providers/Operators of Fintech

5.1 For the purpose of this publication, a provider/operator of Fintech is a person who provides Fintech (e.g. electronic payment applications) for the use by consumers, and/or makes use of Fintech in the provision of financial and related services. A provider/operator of Fintech usually controls, either alone or jointly or in common with others, the collection, holding, processing or use of the personal data that derives from the operation or use of the Fintech. In the circumstances, a provider/operator of Fintech is a data user regulated under the Ordinance. The recommended good practices below seek to assist

[11] The provisions of the Ordinance are binding on data users. DPPs 2(3) and 4(2) in Schedule 1 to the Ordinance impose additional obligations on data users with regard to the retention and security of personal data held by their data processors.

providers/operators in addressing the key privacy risks of Fintech. However, they do not serve to provide a comprehensive guide to compliance with the requirements of the Ordinance.

Transparency

5.2 Providers/operators of Fintech should be transparent about their privacy policies and practices. Plain and user-friendly languages should be adopted in privacy policies to:

(a) explain the types of personal data to be collected, why the collection is necessary, and the consequences if a customer refuses to provide the personal data;

(b identify all intended uses of the personal data;

(c) identify all possible transferees of the personal data (including data processors);

(d) explain users' rights (e.g. a right to access and rectify and a right to opt out of certain uses) and obligations (e.g. an obligation to provide) with respect to their personal data; and

(e) explain the security measures adopted to protect the personal data in transit and storage.

5.3 The above information should be provided by providers/operators of Fintech on or before collection of personal data in the form of Personal Information Collection Statement (**PICS**)[12]. The PICS should be easily readable and understandable in terms of its length, complexity, font size and accessibility.

5.4 In addition to PICS, providers/operators of Fintech must also provide a general statement about their privacy policies and practices in relation to the personal data they handle, i.e. the Privacy Policy Statement (**PPS**). To meet the requirements of openness and transparency under the Ordinance, a PPS must be available to the general public at all times[13].

5.5 In the event that the PICS or PPS are inevitably lengthy (e.g. due to the complexity of the data processing activities), providers/operators of Fintech should display prominently to customers a succinct and easy-to-understand summary of the PICS or PPS[14].

Minimum personal data collection and retention

5.6 Providers/operators of Fintech should collect and retain minimum amount of personal data. Obsolete personal data should be deleted or de-identified in a timely manner.

5.7 Where possible, providers/operators of Fintech should request for personal data only when it is necessary for or directly related to the operation of the Fintech, rather than requiring users to provide personal data of all types of upfront.

Clear and genuine options

5.8 Providers/operators of Fintech should provide clear and genuine options to customers with respect to collection and use of their personal data. For example, for those personal data that is "good to have" rather than necessary for the operation of the Fintech, customers should be provided with clear and genuine options to withhold, and for those uses or disclosures of personal data that are not necessary for or directly related to the operation of the Fintech (e.g. use in personalised advertisements), customers should be provided with clear and genuine options to opt in or opt out.

5.9 An option is clear when it is prominently brought to the attention of the customers, rather than buried in the lengthy privacy policies.

5.10 An option is genuine when the customers' choices will not create significant adverse impact on their access to, and the costs and benefits of the services.

Accuracy of data and reliability of algorithms

5.11 Providers/operators of Fintech, such as credit scoring algorithms, should ensure that the personal data to be used is accurate and impartial. Clarification should be sought from the individuals concerned when the accuracy of the personal data is in doubt.

5.12 Algorithms of Fintech should also be tested for reliability and fairness, in particular when the outcomes of computation will likely have significiant

[12] See footnote 3 above for the transparency requirements under DPP 1(3) in Schedule 1 to the Ordinance.

[13] DPP 5 in Schedule 1 to the Ordinance stipulates that all practicable steps shall be taken by a data user to ensure that a person can-
(a) ascertain the data user's policies and practices in relation to personal data;
(b) be informed of the kind of personal data held by the data user;
(c) be informed of the main purpose for which personal data held by the data user is or to be used.

[14] For detailed guidance on the preparation of PICS and PPS, please refer to the "Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement" issued by the Privacy Commissioner: https://www.pcpd.org.hk//english/resources_centre/publications/files/GN_picspps_e.pdf

impact on the interests, rights and freedoms of the individuals concerned (e.g. credit scores and access to credit facilities). A computational outcome is reliable and fair if it is an objective reflection of the particularities and attributes of the individuals concerned. For example, big data analytics may show that those people who often go out for meals at midnight usually have less savings and are more likely to default in repayment of loans. However, it may well be unfair to apply this observation to the credit assessment of a person who works in night shift (therefore eats at midnight), and accord this person with a low credit score.

5.13 Providers/operators of Fintech should ensure algorithmic transparency by providing individuals with explanations on the automatic assessments and decisions (e.g. credit score) made by Fintech.

Security of data

5.14 Providers/operators of Fintech should ensure both administrative (e.g. policies and procedures) and technical (e.g. logical access control and encryption) security measures are in place to provide adequate safeguards to the personal data in transit and storage, thereby preventing unauthorised or accidental access, processing, erasure, loss or use of the data by either internal staff members or external parties. Generally, the use of commonly accepted information technology security standards and vulnerability scanning are expected.

5.15 Providers/operators of Fintech should develop procedures in relation to handling of data breach incidents. In the events of data breach, providers/operators of Fintech should notify the following parties (where applicable) without delay:

(a) the individuals affected;

(b) law enforcement agencies;

(c) relevant regulators, such as the Privacy Commissioner in the events that personal data is involved, and/or other regulators in relevant areas, such as financial or monetary regulators; and

(d) other stakeholders, such as the financial institutions from which the data in question were collected[15].

Data processors

5.16 When data processors are engaged for the processing and/or storage of personal data, providers/operators of Fintech should adopt contractual and/or other means (e.g. field audit) to ensure that the data processors:

(a) do not retain the personal data longer than necessary;

(b) adopt adequate security measures to protect the personal data;

(c) do not process, use or disclose the personal data for unauthorised purposes; and

(d) notify the providers/operators of Fintech immediately in the events of data breach.

5.17 Providers/operators of Fintech should also be clear about the locations where their data processors store and/or process the personal data. If the storage and/or processing involves transfer of personal data out of Hong Kong, the providers/operators should adopt contractual or other means to ensure that the personal data will have an adequate level of protection at those locations[16].

Privacy Impact Assessment and Privacy By Design

5.18 At or before the development stage of a Fintech, the providers/operators should conduct a privacy impact assessment (**PIA**)[17] to identify and properly address all potential privacy risks in the entire data processing life cycle of the Fintech, i.e. from data collection to storage, processing, use and destruction. Privacy-friendly design and at the outset, default settings should be adopted in the Fintech.

[15] For more details on handling of data breach incidents, please refer to the "Guidance on Data Breach Handling and the Giving of Breach Notifications" issued by the Privacy Commissioner: https://www.pcpd.org.hk//english/resources_centre/publications/files/DataBreachHandling2015_e.pdf

[16] For more details on protecting personal data in cross-border data transfer, please refer to the "Guidance on Personal Data Protection in Cross-border Data Transfer" issued by the Privacy Commissioner: https://www.pcpd.org.hk//english/resources_centre/publications/files/GN_crossborder_e.pdf

[17] For more details on PIA, please refer to the information leaflet "Privacy Impact Assessment (PIA)" issued by the Privacy Commissioner: https://www.pcpd.org.hk//english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf

Download
this publication

Enquiry Hotline : (852) 2827 2827
Fax : (852) 2877 7026
Address : Room 1303, 13/F, Sunlight Tower, 248 Queen’s Road East, Wanchai, Hong Kong
Email : enquiry@pcpd.org.hk

Copyright

Disclaimer

The information and suggestions provided in this publication are for general reference only. They do not serve as an exhaustive guide to the application of the law. The Privacy Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided will not affect the functions and powers conferred upon the Privacy Commissioner under the Personal Data (Privacy) Ordinance.

First published in March 2019