澳 門 特 別 行 政 區 政 府
Governo da Região Administrativa Especial de Macau
個 人 資 料 保 護 辦 公 室
Gabinete para a Protecção de Dados Pessoais

UNOFFICIAL TRANSLATION

Guidelines for Apps Development

When using mobile devices like smart phones, tablet computers, etc, quite often personal data of Macao citizens is collected by app[1] developers or app operators[2]. In some cases, these apps even asked for user authorization to access non-user personal data as stored on the devices. In view of the frequent personal data processing undertaken by app developers and operators, the Office for Personal Data Protection produced this guidance note as a reference for the general public.

I. Application of the Personal Data Protection Act

Should an app developer or app operator, through any apps, accesses, transmits, or uses the user's and non-user's personal data as stored on the mobile device, including collecting information regarding geo-locations, user account(s), contact list(s), etc., processing of information as such is subject to the Personal Data Protection Act (PDPA, or Law 8/2005) according to its Article 4(1)(1) and 3(1).

II. Processing purposes

App developers' or operators' purposes of processing personal data should be directly relating to their provision of app services or functions.

III. Data controller and processor of personal data processing

[1] The apps as indicated in the current guidance note refer to those applications that provide certain services or functions that are operated on smart phones, tablet computers or other mobile devices.
[2] The app developers mentioned in the current guidance note generally refer to the parties that develop, edit and maintain the applications. On the other hand, app operators generally refer to the parties that manage, administer and operate mobile apps. In practice, however, it is difficult to completely differentiate app developers and app operators as they are the same institution, and sometimes not. Aside from app developers and operators, there may also involve other parties. According to Article 4(1)(5) of the PDPA, generally a party is entitled as data controller as long as it could decide for the purposes and methods of the data processing.

UNOFFICIAL TRANSLATION

Under Article 4(1)(5) of the PDPA, 'controller shall mean the natural or legal person, public entity, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data'. In contrast, processor, under Article 4(1)(6) *idem*, shall mean 'a natural or legal person, public entity, agency or any other body which processes personal data on behalf of the controller'.

Generally the app developer, for the app operator's commercial interests, develops apps on the latter's behalf. Even if the app developer could, at its liberty, decide for the best technology and security measures to process personal data, this was originated from the app operator's appointment. In other words, the app developer does not have any rights to decide for the purposes and methods of the personal data processing as it is as a processor. It is, indeed, the app operator to decide for the purposes and the methods of the data processing as it is the data controller. Under certain circumstances, however, if an app developer is also a data controller, then it could decide for the purposes and methods of personal data processing, for instance the app developer itself is also the app operator. On the other hand, when the app developer and app operator jointly decide for the purposes and methods of the personal data processing, as a consequence both of them are regarded as data controllers. One of the examples as such is when the app developer develops an app on behalf of an app operator but at the same time the former also processes personal data for its own interests.

As a consequence it is important for the app developer and app operator to confirm their identities in the data processing. If a party is confirmed as a data controller, this will make its personal data processing subject to the PDPA and it should therefore assume the responsibility stipulated by the PDPA accordingly.

IV. Data processing legitimacy

(I) General personal data

UNOFFICIAL TRANSLATION

1. Collecting and processing users' personal data

Article 6 of the PDPA stipulated the conditions to establish the legitimacy for personal data processing:

(1) the data subject has unambiguously given his consent;

(2) precautionary measures prior to the performance or conclusion of a contract;

(3) for compliance with a legal obligation;

(4) to protect the vital interests of the data subject who is physically or legally incapable of giving his consent;

(5) acting in the public interests or for the legal competence of a public authority;

(6) for pursuing legitimate interests that precedes other interests.

Normally when a data controller processes general personal data, legitimacy could be established under the aforementioned conditions (1) and (2). Under Article 4(1)(9) of the PDPA, explicit consent from a data subject is based on his informed, freely given and specific consent that signified his agreement to the concerned data processing.

When an app is used, normally the app developer or operator processes personal data under two kinds of circumstances, firstly, based on the user's consent — processing legitimacy of the developer or operator only originates from the user's consent. A user's consent, however, is only valid when he has been informed of and freely given his genuine consent to the data processing aimed at specific purposes. In addition, the consent could be withdrawn at any time he wishes. For instance, if a customer could decide whether to provide his data before an app installation or personal data processing taking place, explicit consent is constituted if he still submitted his personal data provided that he had been informed by the data controller that for the app services and functions his personal data would be processed. On the other hand, when using an app, the user's consent is constituted if he submitted his data voluntarily when informed by the data controller that the newly added services or

functions of the app currently in use would process his user data. Secondly, when the app developer or operator laid down in the terms of use of an app that required its users to provide certain types of personal data before certain app services or functions could be used, legitimacy will be established for personal data processing if this user provided his data. Legitimacy as such is established for discharging the contractual terms laid down therein. For example, when installing or running an app, its terms of use asked the user to provide his geo-location information, if he consented to and installed the app, the data controller could then rely on the contract it concluded with him to process his user personal data.

2. Accessing non-user data stored on mobile devices

When a data controller processes non-user information stored on any mobile device, it is also subject to Article 6 of the PDPA, which requires that data processing is based on any of the legitimacy conditions previously mentioned. For instance, according to the terms of use laid down for the instant messaging software it provided, a data controller would access the user's contact list during the provision of services, then data processing legitimacy is based on the performance of contractual terms.

(II) Sensitive data

Under Article 7(1) of the PDPA, 'the processing of personal data revealing philosophical or political beliefs, political society or trade union membership, religion, privacy and racial or ethnic origin, and the processing of data concerning health or sex life, including genetic data, shall be prohibited.' Exceptionally, when a data controller is under circumstances as stipulated in Article 7 of the PDPA, sensitive data could only be processed when special security measures are adopted according to Article 16 of the PDPA, in addition that the non-discrimination principle is at the same time observed. Generally only when a data subject has expressly given his consent then a data controller could process his sensitive personal data. One of the

examples is the special outpatient appointments provided by health care facilities, the data controller could only achieve the legitimacy to process health data as long as a patient has explicitly consented to.

(III) Information relating to unlawful acts

Normally it is unnecessary for a data controller to process any personal data in regard a data subject's unlawful or criminal activities or administrative offenses.

V. Data processing principles

When processing personal data, a data controller must adhere to the principles given in Article 2 and 5 of the PDPA, including the "principles of specific and explicit purposes and lawfulness", "principle of proportionality", as well as the principle governing that "data shall not be kept for longer than is necessary". Data controllers are required to adhere to the principle of proportionality in particular.

Under the principle of proportionality, personal data processing must be 'adequate, relevant and not excessive in relation to the purposes for which it is collected and further processed'. The data collected, therefore, must be necessary to the functions of the app, i.e., the data collected by the app is appropriate to its purposes, in addition that excessive personal data should not be collected and processed. For instance, without collecting the user's geo-location information stored on a mobile device, a restaurant finder app could still recommend the restaurants in the regions or area where the user is interested in. As another example, without the user's authorization if an app, provided by a public authority, has required user's authorization in order to access his contact list and to read contact records, this could be regarded as an unnecessary authorization, with which the information collected is unnecessary for the purposes the app intended to achieve.

VI. Rights of the data subjects

UNOFFICIAL TRANSLATION

Article 10 to 14 of the PDPA guarantee the list of the rights enjoyed by the data subjects, including the right to information, right of access, right to rectify and right to object, etc.

Data controllers should respect the right to information of the data subjects. When collecting personal data through mobile apps, it should formulate declaration, terms of use, or privacy policies that are easy to read, find and understand. To guarantee the right to information as laid down in Article 10 of the PDPA, a data controller should provide to the data subjects information like the identity of the organization, the processing purposes, the type of entity to receive the data, the right to information, right to rectify and the conditions to exercise such rights.

Concurrently with the above, the data controller should also specify its contact information in its apps, in case its user wishes to exercise his right of access.

VII. Data security and confidentiality

(I) Data security

With regard security of personal data processing, Article 15 of the PDPA, which governed the Security of processing, requires data controllers to provide appropriate technical and organizational measures to ensure personal data security.

Moreover, when appointing a data developer, a processor (the party to be appointed) who provides sufficient safeguards in respect of technical security measures and organizational measures should be selected. The relationship between the two parties should be bound by a contract. Meanwhile, the data controller should inspect the implementation of the measures in order to ensure the processor complies with the PDPA. The processor should only be allowed to process data within the scope of the contract and according to the controller's instructions.

Should the processing of an app involve sensitive data or data regarding unlawful or criminal activities or administrative offences, as given in Article 7(2) and 8(1) of

the PDPA, the data controller must adopt special security measures according to Article 16 *idem*.

It should be noted that the system used to process personal data must ensure logical separation of the data concerning health or sex life, including genetic data.

(II) Professional secrecy

According to Article 18 of the PDPA, the data controllers and those who accessed personal data while discharging their duties are covered by professional secrecy even after the duties are finished.

Professional secrecy is a lifelong obligation, requiring those covered by this obligation, even after they left the jobs, to keep confidential the information they obtained when discharging their duties.

When professional secrecy is violated, the involved party is liable to criminal responsibility according to Article 41 of the PDPA; even if it was caused by negligence it is also liable to punishment.

VIII. Data accuracy and retention period

According to Article 5(1)(4) of the PDPA, personal data should be accurate and, where necessary, kept up to date; adequate measures must be taken to ensure that data is inaccurate or incomplete, having regard to the purposes for which it is collected or for which it is further processed, erased or rectified. For example, when an app will access or update the user's contact list, then it should also delete the old contact information.

Also under Article 5(1)(5) of the PDPA, personal data should be kept in a form which permits identification of their subjects for no longer than is necessary for the purposes for which it is collected or for which it is further processed. To this, the data controller should, in its apps, guarantee to remove or delete information.

Whenever a user has reasonably requested to remove the information or his user account has been terminated, unless as otherwise legally stipulated, the data controller should never continue retaining the concerned information, and should completely remove, archive or delete the information accordingly.

In other words, the data controller should maintain the accuracy of the data it processed, and should not retain it for no longer than is necessary for the purposes it intended to achieve.

IX. Formulating policies

Data controllers should formulate policies for processing personal data (for instance, guidelines or processing procedures). While formulating, data controllers should consider the types of the access authorizations it intends to seek from the users, whether authorizations exceed what the users have expected from the scope of services or functions of the app, how the app explained to its users the reasons and the further processing of the personal data it collected, as well as how to ensure the security and confidentiality of the data to be processed, etc. Formulating clear guidelines, terms of use, and privacy policies help users have a better understanding about the data to be collected.

X. Notification obligation

When processing of personal data is under conditions as specified in Article 21 of the PDPA, the data controller should notify the GPDP; otherwise it may constitute administrative offenses.

XI. Conclusion

No doubt apps bring convenience to daily life but when they are used to collect personal data, data controllers should ensure the purposes and the methods established for the data collection, as well as data accuracy, retention period, use of data, data

UNOFFICIAL TRANSLATION

security and confidentially should all be in compliance with the principles of lawfulness and good faith as laid down in the PDPA and other regulations. In addition, particular attention should be devoted to the following:

1) **App developers or operators should process personal data based on the purposes directly relating to the services or functions of the app.**
2) **Legitimacy of personal data processing normally originates from the explicit consent given by the data subjects.**
3) **Data subjects' right to information should be ensured.**
4) **Data processing should be proportional; the data processed should be necessary for the services or functions of the app.**
5) **Data security and confidentiality should be guaranteed.**
6) **Notification obligation should be undertaken.**

Office for Personal Data Protection
September 11th, 2014