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 on Merchants' Processing of Identification Documents of Payment Cardholders

To fulfil the legal obligations laid out in the Guidelines on Money Laundering and the Financing of Terrorism, or for other reasons like transaction security of payment cards, many local merchants, when proceeding payment card[1] transactions, may ask their customers to produce identification documents. Many merchants and customers find it doubtful or disputable whether the said procedure violates the Personal Data Protection Act (hereinafter as "PDPA"), in particular some merchants may collect and register cardholders' identification data during all these transactions. In view of this, the current Guidelines by the Office for Personal Data Protection (hereinafter as "GPDP") intend to be a reference to all sectors of the community.

## I. Application of the Personal Data Protection Act

According to Articles 4(1)(1) and 3(1) of Law 8/2005(PDPA), customers' identification document data collected by merchants and its post-processing should be regulated by the law.

## II. Purposes of Data Processing

Within the current Guidelines, for merchants to collect and register cardholders' identification data and to further process it, it should serve the purposes of:

[1] In the current Guidelines, "payment cards" refer to those the multi-purpose cards under the multi-purpose payment scheme that offer credit or debit facilities for settling transactions of goods or services through the payment networks, including multi-purpose stored value cards.

1. Complying with the obligations given by Law 2/2006 (Prevention and Suppression of the Crime of Money Laundering) and Law 3/2006 (Prevention and Suppression of the Crime of Terrorism), and abiding by the relevant guidelines set out by the related supervisory institutions in Macao (hereinafter as the "Guidelines on Money Laundering and the Financing of Terrorism").[2]

2. Ensuring the transaction security of payment cards.

The current Guidelines are aimed at the personal data processing held for the above purposes. The current Guidelines do not apply to cases wherein merchants collect cardholders' identification data for other purposes (for instance, a hotel registering customer data for room arrangement).

## III. Legitimacy of Data Processing

Legitimacy for the processing of personal data is given in Article 6 of the PDPA.

### 1. Legitimacy in Collecting and Registering Data

Generally merchants could only collect and register cardholders' identification document data given the data subject gave his unambiguous consent.

According to Article 4(1)(9) of the law last mentioned, a data subject's unambiguous consent should mean this person has been informed when freely giving his specifically indicated wishes, whereby consent is given to the concerned processing. Therefore, if the cardholder has been informed that his identification data is collected by a merchant for the purposes mentioned in Point II above, in conjunction that the data subject is willing to

[2] For the purpose as stated in Point 2 above to collect and register customers' data, the customers concerned are referred to those given in Article 7(1)(1) of Law 2/2006 and Article 11 of Law 3/2006, but excluding any persons who are the parties concluded a contract or the gamblers as referred in the said laws.

continue the transaction followed by handing his identification document to the merchant for registration, then this is regarded as giving unambiguous consent.

On the contrary, if a data subject refuses to continue the transaction or refuses to submit his identification document to the merchant for registration, it is deemed as consent is not given by the cardholder. As a consequence, the merchant should not collect I.D. data from this cardholder. Under this circumstance, the merchant has to evaluate the legal and security risks from the payment card transaction, before deciding whether or not to continue the transaction. As in line with the related regulations given in Article 7 (1)(3) of Law 2/2006 and Article 11 of Law 3/2006, both specify that if a data subject refuses to provide data, then the merchant should refuses to carry out any activities.

As a wide variety of payment cards are accepted in Macao, different laws may apply as card issuers come from different countries and regions. Under special circumstances, the payment card which a client holds could have special provisions, for example, the contract concluded between the cardholder and the card issuer stipulates that the former has to provide identification data to the merchant for certain transactions. Despite the legitimacy, as given in Article 6(1) of the PDPA, in personal data processing could arise from the "contract performance", GPDP is of the opinion that, as situation changes all the time, it is safer and more feasible for merchants to first acquire the data subject's unambiguous consent. If the cardholder refuses to provide his identification data, he should aware that, subject to the contract concluded between him and the issuer, the transaction will not be accepted.

## 2. Legitimacy in the Post-processing of Data

As regards the cardholders' identification data the merchants collected, generally it will be kept for a period of time and might be provided to relevant organizations according to law.

Given that the data subject has already given his unambiguous consent to the collection and registration of his data, hence its post-processing is deemed to be based upon the said unambiguous consent. In addition, data processing like storage, forwarding, and so forth, which is taken in conformity with Guidelines on Money Laundering and the Financing of Terrorism; or passing data to enforcement authorities, acquiring banks or card issuers in cases of fraudulent transactions, and so forth, legitimacy in both these cases arises from the "fulfilment of legal obligations" given in Article 6(2) or from the "legitimate interests" in Article 6(5) of the of the PDPA.

## IV. Proportionality of Data Processing

For the principles of personal data processing, a number of which have been laid down in Article 5 of the PDPA, including the principle of purpose and the principle of proportionality. In other words, a merchant should collect personal data for specific, explicit, legitimate purposes and to which his activities are directly related, and the post-processing should not depart from such purposes as well. Data collection and processing should be appropriate and in proportion, without exceeding the purposes of data collection and post-processing.

Therefore, based on the purposes referred in Point II of the current Guidelines, merchants should not in all transactions collect and register cardholders' identification documents. Generally speaking, only under the following circumstances merchants can undertake collection:

1. In situations where Guidelines on Money Laundering and the Financing of Terrorism requires registering customers' data in certain transactions, otherwise no transactions should be carried out; as such the merchants could make the collection.

UNOFFICIAL TRANSLATION

2. Some payment cards are subject to special transaction security regulations, which require merchants of certain types or of certain businesses to collect cardholders' data under certain circumstances; otherwise transaction should not be processed. Such requirement imposed on merchants is usually made by the payment card organizations, acquiring banks, etc. Merchants from those businesses involving anti-money laundering and anti-terrorism financing, or prone to be abused by the law-breakers for payment card crimes, more likely they have to undertake the said requirement. When a cardholder is using a payment card to settle a transaction whereby is deemed as a situation aforementioned, then the merchant is allowed to collect data.
3. In many security regulations for payment card transactions, merchants are obliged to undertake responsibilities to verify the authenticity of payment cards and cardholders. If there is an obvious indication of doubts over a cardholder's identity or the authenticity of the payment card, the merchant can collect the data, for instance, an apparent male customer using a payment card that should belong to a female cardholder. Generally speaking, merchants who are regulated by the Guidelines on Money Laundering and the Financing of Terrorism, and merchants of certain types or of certain businesses to whom the related security regulations for payment card transactions apply, as subject to higher fraud risks, they are more likely to collect cardholders' identification data.

Under the circumstances referred in Points 1 and 2 aforementioned, merchants processing personal data are mainly to adhere with the guidelines and requirements of the supervisory institutions, card payment organizations, acquiring banks, etc. The merchants should organize and prepare well these guidelines and requirements, and provide appropriate staff trainings, so staff members could better follow these regulations, which could also be used as reference in case of any GPDP's investigations of personal data processing.

UNOFFICIAL TRANSLATION

In respect of the types of data to be collected, in GPDP's views, one should comply with the principle of minimal intervention, i.e., collecting the necessary data only. The mentioned guidelines and requirements have put forward the general specifications for data collection. Even under circumstances as noted in Point 3 last said, the types of data collected should not exceed what the payment card organizations and acquiring banks demand as mentioned in Point 2. If the requirements the payment card organizations and acquiring banks, and so forth, laid down, as referred in Point 2, have not clearly identified the types of data, the types of the data collected should not exceed those required by the supervisory institutions as noted in Point 1 above.

With regard to collecting and post-processing data, GPDP reminds merchants of the following:

1. Except as otherwise specified, identification document copies should not be collected. To GPDP's knowledge, currently the guidelines and requirements given by supervisory institutions, card payment organizations, acquiring banks, etc., normally do not expressly stipulate merchants to collect identification document copies from customers using payment cards for their transactions. If otherwise specified in the said guidelines and requirements, GPDP will analyze the case based on the proportionality principle.
2. Except as required by Guidelines on Money Laundering andthe Financing of Terrorism or guidelines by other competent institutions to record complete identification numbers, generally this should not be collected as such, thereby "X" can be used to replace at least two digits.
3. Using automatic means to record relevant identification data should be avoided. As this kind of data recording may imply the transaction is subject to supervision or high risks, or may indicate suspicion about the authenticity of the payment card or its holder.

Using automatic means to record the identification data not only poses potential threats to or affects the data subjects' interests or rights, also the concerned organizations may have to face higher information security risks, for instance, information leaks caused by computer hacking.

4. Except as specifically stipulated in the Guidelines on Money Laundering and the Financing of Terrorism or in the guidelines issued by payment card organizations, acquiring banks, and so forth, data of customer's identification and payment card transactions should be kept separately. If stored together, from the perspective of payment card data security, customer's identification data and payment card data, both being independent data of low risks nature, combined into a kind of high risk data, which is prone to be targeted by law-breakers. If this combined data is leaked, data subjects' rights and interests will be more potentially affected and at higher risks, including the risk of payment card security.

## V. Data Security and Duration of Data Retention

Merchants are obliged to ensure data processing security. Since merchants have already set out measures for the security of transaction data, GPDP recommends merchants protect other personal data arises from transactions appropriately, by referring to measures for the security of transaction data that is already in place. Except when supervisory institutions, payment card organisations, or acquiring banks, etc., in their guidelines and requirements, or laws, set forth data forwarding, no third parties should be forwarded. When collecting data, it is best to use specialized independent forms, in order to avoid any inconsistent methods, which may pose threats to data security, of collecting and retaining the concerned data.

Trainings and reminders should be constantly provided to employees, reminding them to strictly abide by the regulations for information security the merchants imposed and to comply

with their duties of professional secrecy. For example, staff members should be informed that any violations of the PDPA caused by failing the obligation of professional secrecy or accessing information improperly, they could be imposed with maximum three years of imprisonment. Likewise, anyone's improper handling of data during data processing could also damage the merchants' interests, or even found liable to legal responsibilities.

Pursuant to Article 5(1)(5) of the PDPA, only during the period designed to achieve data collection or post-processing purposes, data should be kept in a form which permits identification. Therefore, merchants should set out a retention period, and should preserve the data within a reasonable period that fulfils the purposes of data processing. The justifications for merchants to set out a data retention period are mainly based on: relevant laws and legal provisions(for example, Law 2/2006 and Law 3/2006, etc.), guidelines issued by the competent institutions(including the relevant Guidelines on Money Laundering and the Financing of Terrorism, or guidelines or requirements issued by payment card organizations, acquiring banks, etc.).

1. Merchants should follow the retention period(i.e. the maximum retention period) for which laws, legal provisions, or guidelines stipulated.
2. Merchants should set forth a maximum retention period based on the relevant purposes of data processing if laws, legal provisions, or guidelines only stipulate the minimum retention period. Normally the maximum retention period expires three months after the minimum retention period ended.
3. In case data of judicial proceedings is involved, a special retention period could be established, but normally data should be destroyed six months after a judgement has become definite.

## VI . Rights of Data Subject

The rights of data subjects are provided for in Articles 10 to 14 of the PDPA. Merchants should ensure the rights, especially the right to information, of the data subjects in accordance with the law.

Merchants should, according to Article 10 of the PDPA, adopt a Personal Data Collection Statement which allows the cardholder(s) whose information is collected to have access to. At the same time, prior to the collection of identification information from a cardholder, it should ensure that the data subject has been informed of the purposes of data processing.

It is a good practice for a merchant to establish his own specialized, independent forms, in which a "Personal Data Collection Statement" is contained. Such forms should be filled by the cardholder(s) before it is verified by the merchants. After the cardholder(s) understood the collection purposes and the content of the form, the merchants' staff could help filling it if asked by the cardholder(s).

## VII. Summary

The Personal Data Protection Act has set out the legal regime for personal data processing and protection. When merchants collect and process the identification data of cardholder(s), they should strictly abide by the PDPA, in particular to the following:

1. **The processing purposes laid out in the current Guidelines should be limited to the compliance of legal obligations given in the Guidelines on Money Laundering and the Financing of Terrorism, or ensuring the security of payment card transactions.**
2. **The legitimacy to collect and record personal data should be based on the unambiguous consent of the data subject.**

UNOFFICIAL TRANSLATION

3. **Data collection should be appropriate, and no excessive data should be collected, in particular no identification copies should be collected when there are no sufficient grounds.**
4. **Security and confidentiality of the data should be ensured.**
5. **Data subjects' right to information should be ensured.**

The current Guidelines aim to provide practical recommendations to merchants, and to clarify queries from a legal and practical point of view and attempt to provide reference to all sectors of the community. Each merchant, being an entity responsible for personal data processing, should set out a policy for personal data processing after considering its own circumstances, so as to adhere to the obligations given in the Personal Data Protection Act. GPDP also encourages the payment card organizations and acquiring banks to jointly set up relevant guidelines, rules and good practices in order to better safeguard the interests of all parties.

Office for Personal Data Protection

17th April, 2013

Annex I: Q&A

Annex II: Personal Data Collection Statement (sample)

UNOFFICIAL TRANSLATION

Annex I

# Guidelines on Merchants' Processing of Identification Documents of Payment Cardholders

## Q&A

The content of the current Q&A is based on the Guidelines on Merchants' Processing of Identification Documents of Payment Cardholders. Its application is limited to the personal data processing as referred in the same document.

Q1: Are merchants in all transactions allowed to collect and register cardholders' identification document data?
A: Normally they are not allowed. Please refer to the principle of proportionality in data processing, as laid out in Point 4 of the titled Guidelines.

Q2. Apart from the data processing purposes given in the Guidelines, are merchants allowed to collect and register identification data for other purposes?
A: Yes, for example, hotels register customers' data for room arrangement. It should be noted that the Guidelines only apply to the legal obligations given in Law 2/2006 and Law 3/2006 for the compliance with those related guidelines issued by the supervisory institutions, and to process personal data by ensuring transaction security of payment cards; but not for data processing of other purposes.

Q3: Could merchants provide the data collected and registered to the competent institutions?
A: Yes. When complying with the Guidelines on Money Laundering and the Financing of Terrorism, or forwarding or providing data to competent institutions because of any fraudulent payment card transactions, etc., consequentially data processing legitimacy arises from the "fulfilment of legal obligations" or "legitimate interests", as found in Article 6(2) and Article 6(5) of the PDPA respectively.

Q4: Is it only when unambiguous consent is received, merchants are allowed to collect and register cardholders' identification data?

A: Merchants generally could only collect and register a cardholder's identification data upon his unambiguous consent. Identification data from a customer should not be collected, if he refuses to continue the transaction or refuses to submit his identification document for registration by the merchant.

Q5: To continue with the previous question, when a data subject disagrees and a merchant is obliged to discern, how should this be handled?

A: In accordance with the relevant provisions of Law 2/2006 and Law 3/2006, to fulfil the obligations concerning anti-money laundering and anti-terrorism financing, merchants should ask customers for their identification data according to the concerned provisions. For instance, when there are signs of possible money laundering or terrorism financing, or when there involves large-amount transactions.

A merchant should not collect identification data from a cardholder if he disagrees so. Then, the merchant should evaluate the legal and security risks from the payment card transaction, for instance, whether to refuse the transaction or not. As also referred in Article 7(1)(3) of Law 2/2006 and Article 11 of Law 3/2006, a merchant should abstain from all activities if a data subject disagrees to provide his data.

Q6: What is the principle of minimal intervention? How should a merchant process data to avoid violating the principle of proportionality?

A: The principle of minimal intervention means when someone processes personal data, he should only process the data that is necessary for achieving the purposes needed, and beyond which violates the principle of proportionality. For example, unless law, legal provisions, or guidelines specify, no ID copies should be collected.

Q7. To continue with the previous question, should merchants not to collect ID copies under all circumstances?

A: No. A merchant could collect ID copies if it is expressly provided for. But in case only specified by guidelines or requirements from supervisory institutions, payment card

organisations or acquiring banks, the GPDP will analyse, with the principle of proportionality, on a case-by-case basis.

Generally speaking, in collecting ID copies the principle of proportionality is possibly met only when involving payment cards issued by countries or areas outside Macao and where the local laws there or the guidelines of the supervisory institutions there set forth, or the contract concluded between the card issuers and the cardholder(s) stipulated the latter, for certain transactions, have to provide his ID copies to the former. The precondition is that, after all, these requirements do not violate the PDPA.

Also to be noted is merchants should find out whether the said collection of ID copies is mandatory. If only optional, the merchant should consider whether it is necessary to collect.

Q8: What does avoiding recording identification data by automatic means refer to?

A: This refers to avoid using automatic means, for example, computer, to record the identification data collected from cardholder(s). This could mean the transaction proceeded is subject to monitoring or high risks, or could imply suspicion over the authenticity of the cardholder(s) or the payment card(s). Such recording not only poses potential influence or risks to the cardholders' interests or rights, also the concerned institutions have to bear higher risks and serious consequences for their information security, particularly data leakage caused by illegal system hacking.

Q9: How to establish a retention period? What is the minimum period mentioned in the Guidelines?

A: According to Article 5(1)(5) of the PDPA, only during the period designed necessary for the data-collection or post-processing purposes data should be retained. In other words, merchants should devise a retention period for achieving the data processing purposes.

When laws, legal provisions, or guidelines do not stipulate for such a period, the data controllers should, according to the time needed to achieve the processing purposes, devise a data retention period. Contrarily, controllers could comply with the stipulations given in the relevant laws, legal provisions, or guidelines.

The minimum retention period is referred as the minimum period which a merchant

should retain the data. If laws, legal provisions, or guidelines stipulated the minimum retention period, merchants should devise the maximum retention period for the concerned data processing purposes, normally such period ends three months after the minimum period expires.

For any questions about the retention period, merchants are recommended to inquire the relevant institutions.

Q10: How could merchants ensure the right to information of data subjects?

A: Article 10 of the PDPA regulates the right to information of data subjects. To satisfy and ensure such a right, one of the methods is to adopt a Personal Data Collection Statement, which is also a legal obligation of data controllers. The content of the right to information aims to inform the data subjects about the controllers' identity and processing purposes, etc, which are simple and general information. Such information includes, for instance, the identity of the organisations, processing purposes and the data recipients.

Q11: To continue with the previous question, whether the provision of the right to information means allowing revealing facts of offences to customers or any third persons?

A: No. As mentioned above, right to information aims to inform the data subject of simple, general information, like data controllers' identities, purposes, etc. As a consequence, this does not involve any particular case and has no relations to reporting facts of offences. In fact, according to Article 7(4) of Law 2/2006 and Article 11 of Law 3/2006, it is forbidden for anyone to reveal any facts, which someone aware of while performing his duties and are related to the legal obligations given in paragraphs (5) and (6) of Article 7(1), Law 2/2006, to his customers or any third parties.

Annex II

Declaration of the Office for Personal Data Protection

This sample below is for reference only. Merchants should formulate their own "Personal Data Collection Statement" in accordance with their own specific processing circumstances.

# Personal Data Collection Statement

# by (Merchant XX)

# (sample)

To fulfill the legal obligations and ensure transaction security of payment cards, we may require proof of identity by asking identification documents from a customer who settles his/her transaction with a payment card. In addition, we may also record some of his/her identity details. The processing of such personal data is regulated by the Personal Data Protection Act and other related laws. Data recipients are limited to acquiring banks, card issuers, and those entities shall be informed according to laws. If a customer refuses to comply with these requirements, we may refuse to process such payment card transaction.