THE MACAO SPECIAL ADMINISTRATIVE REGION

Act 8/2005

Personal Data Protection Act

Under Article 71 (1) of the Basic Law of the Macao Special Administrative Region, the Legislative Council hereby decrees the following to implement the fundamental order established by Articles 30, 32, and 43 of the Basic Law of the Macao Special Administrative Region.

CHAPTER I
General provisions

Article 1
Object

This Act establishes the legal system on the processing and protection of personal data.

Article 2
General principle

The processing of personal data shall be carried out transparently and in strict respect for privacy and for other fundamental rights, freedoms and guarantees enacted in the Basic Law of the Macao Special Administrative Region, the instruments of international law and the legislation in force.

Article 3
Scope

1 – This Act shall apply to the processing of personal data wholly or partly by automatic means, and to the processing other than by automatic means of personal data which form part of manual filing systems or which are intended to form part of manual filing systems.
2 – This Act shall not apply to the processing of personal data carried out by a natural person in the course of a purely personal or household activity, save those with the purposes of systematic communication and dissemination.
3 – This Act shall apply to video surveillance and other forms of capture, processing and dissemination of sound and images allowing persons to be identified, provided the controller is domiciled or based in the Macao Special Administrative Region (the MSAR)

or makes use of a computer or data communication network access provider established on the MSAR territory.

4 – This Act shall apply to the processing of personal data regarding public safety without prejudice to special rules in instruments of international law and inter-regional agreements to which the MSAR is bound and specific laws pertinent to public safety and other related regulations.

Article 4

Definitions

1 – For the purposes of this Act:

(1) "personal data" shall mean any information of any type, irrespective of the type of medium involved, including sound and image, relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an indication number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(2) "data subject" shall mean the natural person whose data are processed;

(3) "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(4) "personal data filing system" ("filing system") shall mean any structured set of personal data which are accessible according to specific criteria, regardless of the form or method of its establishment, storage and organization;

(5) "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;

(6) "processor" shall mean a natural or legal person, public entity, agency or any other body which processes personal data on behalf of the controller;

(7) "third party" shall mean any natural or legal person, public entity, agency or any other body other than the data subject, the controller, the processor and the persons under the direct authority of the controller or the processor, which are qualified to process the data;

(8) "recipient" shall mean a natural or legal person, public entity, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a law or a statutory regulation with organizational nature shall not be regarded as recipients;

(9) “the data subject’s consent” shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed;

(10)“combination of data” shall mean a form of processing which consists of the possibility of correlating data in a filing system with data in a filing system or systems kept by another or other controllers or kept by the same controller for other purposes;

(11)“public authority” shall mean an entity to which No. 3 of Article 79 of the Civil Code refers;

(12)“statutory regulation with organizational nature” shall mean a provision in law regulating the organization and function, or in the statute, of any entity that is competent to process the personal data or carry out other actions enacted in this act.

2 – To serve (5) above, if the purpose and method are determined in the law or statutory regulation with organizational nature, the controller shall be designated in it.

CHAPTER II
Processing and quality of personal data and the lawfulness of their processing

Article 5
Data quality

1 – Personal data must be:

(1) processed lawfully and with respect for the principle of good faith and the general principle in Article 2;

(2) collected for specified, explicit, legitimate purposes and for purposes directly related to the activity of the controller; and not further processed in a way incompatible with those purposes;

(3) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(4) accurate and, where necessary, kept up to date; adequate measures must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(5) kept in a form which permits identification of their subjects for no longer than is necessary for the purposes for which they were collected or for which they are further processed.

2 – The storing of data for historical, statistical or scientific purposes for longer periods than in (5) above may be authorised by the public authority at the request of the controller in the case of a legitimate interest.

Article 6

Criteria for making data processing legitimate

Personal data may be processed only if the data subject has unambiguously given his consent or if processing is necessary:

(1) for the performance of a contract or contracts to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract or a declaration of his will to negotiate;

(2) for compliance with a legal obligation to which the controller is subject;

(3) in order to protect the vital interests of the data subject if the latter is physically or legally incapable of giving his consent;

(4) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;

(5) for pursuing the legitimate interests of the controller or the third party to whom the data are disclosed, except where such interests should be overridden by the interests for fundamental rights, freedoms and guarantees of the data subject.

Article 7

The processing of sensitive data

1 – 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.

2 – With guarantees of non-discrimination and with the security measures provided for in Article 16, the processing of the data referred to in the previous number shall be carried out when one of the following conditions applies:

(1) when the processing of the data referred to in the previous number is given explicit authorisation by a legal provision or by a statutory regulation with organizational nature;

(2) when, on important public interest grounds, such processing is essential for exercising the legal or statutory rights of the controller, and authorised by the public authority;

(3) when the data subject has given his explicit consent for such processing.

3 – The processing of the data referred to in No. 1 shall also be carried out when one of the following conditions applies:

(1) when it is necessary to protect the vital interests of the data subject or of another person, and the data subject is physically or legally incapable of giving his consent;
(2) when it is carried out with the data subject's consent in the course of its legitimate activities by a legal person or non-profit seeking body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;
(3) when it relates to data which are manifestly made public by the data subject, provided his consent for their processing can be clearly inferred from his declarations;
(4) when it is necessary for the establishment, exercise or defence of legal claims and is exclusively carried out for that purpose.

4 – The processing of data relating to health and sex life, including genetic data, shall be carried out if it is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, provided those data are processed by a health professional bound by professional secrecy or by another person also subject to an equivalent obligation of secrecy, and it is notified to the public authority under Article 21, and where suitable safeguards are provided.

Article 8

Suspicion of illegal activities, criminal and administrative offences

1 – Central registers relating to persons suspected of illegal activities, criminal and administrative offences and decisions applying penalties, security measures, fines and additional penalties may only be created and kept by public services vested with that specific responsibility by a legal provision or a statutory regulation with organizational nature, subject to observance of procedural and data protection rules in force.

2 – The processing of personal data relating to persons suspected of illegal activities, criminal and administrative offences and decisions applying penalties, security measures, fines and additional penalties may be carried out, subject to observance of the rules for the protection of data and the security of information, when such processing is necessary for pursuing the legitimate purposes of the controller, provided the fundamental rights and freedoms of the data subject are not overriding.

3 – The processing of personal data for the purposes of police investigations shall be restricted to the processing necessary to prevent a specific danger or to prosecute a particular offence and to exercise the responsibilities provided for in a legal provision, in a statutory regulation with organizational nature, or in the terms of instruments of international law or inter-regional agreements applicable in the MSAR.

Article 9

Combination of personal data

1 - The combination of personal data not provided for in a legal provision or a statutory regulation with organizational nature shall be subject to the authorisation of the public authority, requested by the controller or jointly by the corresponding controllers under No. 1 of Article 22.

2 - The combination of personal data must:

(1) be necessary for pursuing the legal or statutory purposes and legitimate interests of the controller;

(2) not involve discrimination or a reduction in the fundamental rights and freedoms of the data subjects;

(3) be covered by adequate security measures;

(4) take account of the type of data subject to combination.

CHAPTER III

Rights of the data subject

Article 10

Right to information

1 – The controller or his representative shall provide a data subject from whom data relating to himself are collected with the following information, except where he already has it:

(1) the identity of the controller and of his representative, if any;

(2) the purposes of the processing;

(3) other information such as:

(i) The recipients or categories of recipients;

(ii) Whether replies are obligatory or voluntary, as well as the possible consequences of failure to reply;

(iii) The existence and conditions of the right of access and the right to rectify, provided they are necessary, taking account of the specific circumstances of collection of the data in order to guarantee the data subject that they will be processed fairly.

2 – The documents supporting the collection of personal data shall contain the information set down in the previous number.

3 – If the data are not collected from the data subject and except where he already has it, the controller or his representative must provide the data subject with the information set

down in No. 1 at the time of undertaking the recording of data or, if a disclosure to third parties is envisaged, no later than the time the data are first disclosed.

4 – If data are collected on open networks the data subject shall be informed, except where he is already aware of it, that personal data relating to him may be circulated on the network without security measures and may be at risk of being seen and used by unauthorised third parties.

5 – The obligation to provide information may be waived by any one of the following:

(1)a legal provision;

(2)on the grounds of security and criminal prevention or investigation;

(3)in particular for processing for statistical purposes or for the purposes of historical or scientific research, when the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law or administrative regulations, in which case notification to the public authority is required.

6 – With respect to the basic right of the data subject under No. 3 of the next article, the obligation to provide information under this Article shall not apply to the processing of data carried out solely for journalistic purposes or the purpose of artistic or literary expression.

Article 11

Right of access

1 – The data subject has the right to obtain from the controller without constraint at reasonable intervals and without excessive delay or expense:

(1) Confirmation as to whether or not data relating to him are being processed and information as to the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed;

(2) Communication in an intelligible form of the data undergoing processing and of any available information as to their source;

(3) Knowledge of the reason involved in any automatic processing of data concerning him;

(4) The rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Act, in particular because of the incomplete or inaccurate nature of the data;

(5) Notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (4), in which case the third parties are required to rectify, erase or block the data accordingly, unless this proves impossible, or would involve a disproportionate effort.

2 – In the case of the processing of personal data relating to security and criminal prevention or investigation, the right of access may be exercised by means of the competent authority in that case.
3 – In the cases provided for in No. 6 of the previous article, the right of access is exercised by means of the public authority, securing the rules applicable, in particular those guaranteeing freedom of expression and information, freedom of the press and the professional independence and secrecy of journalists.
4 – In the cases provided for in No. 2 and No. 3, if communication of the data might prejudice security, criminal prevention or investigation and freedom of expression and information or the freedom of the press, the competent authority in that case or the public authority shall only inform the data subject of the measures taken within the limits of maintaining the targeted value of protection described in this number.
5 – The right of access to information relating to health data, including genetic data, is exercised by means of the doctor chosen by the data subject.
6 – If the data are not used for taking measures or decisions regarding any particular individual, the law may restrict the right of access where there is clearly no risk of breaching the fundamental rights, freedoms and guarantees of the data subject, particularly the right to privacy, and when the data are used solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

Article 12

Right to object

1. Save where otherwise provided by law, the data subject has the right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, and where there is a justified objection the processing instigated by the controller may no longer involve those data;
2. The data subject also has the right to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing or any other form of commercial research, or to be informed before personal data are disclosed for the first time to third parties for the purposes of direct marketing or for use on behalf of third parties, and to be expressly offered the right to object free of charge to such disclosure or uses.

Article 13

Right not to be subject to automated individual decisions

1 – Every person shall have the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on

automated processing of data intended to evaluate certain personal aspects relating to him, in particular his performance at work, creditworthiness, reliability or conduct.

2 – Without prejudice to compliance with the other provisions of this Act, a person may be subject to a decision taken under No. 1:

(1) if that decision is taken in the course of the entering into or performance of a contract, provided that the request for the entering into or the performance of the contract has been satisfied, or that there are suitable measures to safeguard his legitimate interests, particularly arrangements allowing him to put his point of view.

(2) if that decision is authorised by a legal provision which shall lay down measures to safeguard the data subject's legitimate interests.

Article 14

Right to indemnification

1 –Any person who has suffered damage as a result of an unlawful processing operation or of any other act incompatible with legal provisions or regulations in the area of personal data protection is entitled to receive compensation from the controller for the damage suffered.

2 – The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

3 – If a processor involves, Article 492 of the Civil Code and its following provisions pertinent to relation of commission shall apply.

CHAPTER IV

Security and confidentiality of processing

Article 15

Security of processing

1 – The controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2 – Where processing is carried out on his behalf the controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures.

3 – The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller and that the obligations referred to in No. 1 shall also be incumbent on the processor.

4 – Proof of the will to negotiate, the contract or the legal act relating to data protection and the requirements relating to the measures referred to in No. 1 shall be in writing in a document legally certified as affording proof.

Article 16

Special security measures

1 - The controllers of the data referred to in No. 2 of Articles 7 and Article 8 shall take appropriate measures to:

1) prevent unauthorised persons from entering the premises used for processing such data (control of entry to the premises);
2) prevent data media from being read, copied, altered or removed by unauthorised persons (control of data media);
3) prevent unauthorised input and unauthorised obtaining of knowledge, alteration or elimination of personal data input (control of input);
4) prevent automatic data processing systems from being used by unauthorised persons by means of data transmission premises (control of use);
5) guarantee that authorised persons may only access data covered by the authorisation (control of access);
6) guarantee the checking of the bodies to whom personal data may be transmitted by means of data transmission premises (control of transmission);
7) guarantee that it is possible to check *a posteriori* , in a period appropriate to the nature of the processing, the establishment in the regulations applicable to each sector of which personal data are input, when and by whom (control of input);
8) in transmitting personal data and in transporting the respective media, prevent unauthorised reading, copying, alteration or elimination of data (control of transport).

2 – Taking account of the nature of the bodies responsible for processing and the type of premises in which it is carried out, the public authority may waive the existence of certain security measures, subject to guaranteeing respect for the fundamental rights, freedoms and guarantees of the data subjects.

3 – The systems must guarantee logical separation between data relating to health and sex life, including genetic data, and other personal data.

4 – Where circulation over a network of the data referred to in Article 7 may jeopardise the fundamental rights, freedoms and guarantees of their data subjects the public authority may determine that transmission must be encoded.

Article 17

Processing by a processor

Any person acting under the authority of the controller or the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 18

Professional secrecy

1 – Controllers and persons who obtain knowledge of the personal data processed in carrying out their functions shall be bound by professional secrecy, even after their functions have ended.

2 –Officers, agents or staff who act as consultants for the public authority shall be subject to the same obligation of professional secrecy.

3 – The provision in the previous numbers shall not exclude the duty to supply the obligatory information according to the law, except when it is contained in filing systems organised for statistical purposes.

CHAPTER V

Transfer of personal data outside the MSAR

Article 19

Principles

1 - The transfer of personal data to a destination outside the MSAR may only take place subject to compliance with this Act and provided the legal system in the destination to which they are transferred ensures an adequate level of protection.

2 – The adequacy of the level of protection referred to in the previous number shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the place of origin and place of final destination, the rules of law, both general and sectoral, in force in

the destination in question and the professional rules and security measures which are complied with in that destination.

3 – It is for the public authority to decide whether a legal system ensures an adequate level of protection referred to in the previous number.

Article 20

Derogations

1 - A transfer of personal data to a destination in which the legal system does not ensure an adequate level of protection within the meaning of No. 2 of the previous article may be allowed on condition that the public authority is notified, and that the data subject has given his consent unambiguously to the proposed transfer, or if that transfer:

(1) is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request;

(2) is necessary for the performance or conclusion of a contract concluded or to be concluded in the interests of the data subject between the controller and a third party;

(3) is necessary or legally required on important public interest grounds, or for the establishment, exercise of defence of legal claims;

(4) is necessary in order to protect the vital interests of the data subject;

(5) is made from a register which according to laws or administrative regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, provided the conditions laid down in law for consultation are fulfilled in the particular case.

2 – Without prejudice to No. 1 the public authority may authorise a transfer or a set of transfers of personal data to a destination in which the legal system does not ensure an adequate level of protection within the meaning of No. 2 of the previous article, provided the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and with respect to their exercise, particularly by means of appropriate contractual clauses.

3 – A transfer of personal data which is necessary for the protection of defence, public security and public health, and for the prevention, investigation and prosecution of criminal offences, shall be governed by special legal provisions or by the international conventions and regional agreements to which the MSAR is party.

CHAPTER VI
Notification

Article 21
Obligation of notification

1 – The controller or his representative, if any, must notify the public authority in written form within eight days after the initiation of carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2 – The public authority may authorise the simplification of or exemption from notification for particular categories of processing which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of the data subjects and to take account of criteria of speed, economy and efficiency.

3 – The authorisation, which must be published in the *Official Gazette of the MSAR*, must specify the purposes of the processing, the data or category of data to be processed, the category or categories of data subjects, the recipients or categories of recipients to whom the data may be disclosed and the length of time the data are to be stored.

4 – Processing whose sole purpose is the keeping of a register which according to laws or administrative regulations is intended to provide information to the public and which is open to consultation by the public in general or by any person demonstrating a legitimate interest shall be exempted from notification.

5 – The non-automatic processing of the personal data provided for in No. 1 of Article 7 shall be subject to notification when they are processed under No. 3 (1) of that Article.

Article 22
Prior checking

1 – Save where otherwise referred to in No. 2, the authorisation of the public authority is required for:

(1) the processing of personal data referred to in No. 2 of Article 7;

(2) the processing of personal data relating to credit and the solvency of the data subjects;

(3) the combination of personal data provided for in Article 9;

(4) the use of personal data for purposes not giving rise to their collection.

2 – The processing referred to in the previous number may be authorised by legal provisions or statutory regulations with organizational nature, in which case it does not require the authorisation of the public authority.

Article 23

Content of applications for opinions or authorisation and notification

Applications for opinions, authorisation and notifications submitted to the public authority shall include the following information:

(1) the name and address of the controller and of his representative, if any;

(2) the purposes of the processing;

(3) a description of the category or categories of data subjects and of the data or categories of personal data relating to them;

(4) the recipients or categories of recipients to whom the data might be disclosed and in what circumstances;

(5) the body entrusted with processing the information, if it is not the controller himself;

(6) any combinations of personal data processing;

(7) the length of time for keeping personal data;

(8) the form and circumstances in which the data subjects may be informed of or may correct the personal data relating to them;

(9) proposed transfers of data to third countries;

(10) a general description enabling a preliminary assessment to be made of the adequacy of the measures taken under Articles 15 and 16 to ensure security of processing.

Article 24

Obligatory information

1 – The legal provisions or statutory regulations with organizational nature referred to in No. 2 of Article 7 and No. 1 of Article 8, the authorisations of the public authority and the register of personal data processing must indicate at least:

(1) the controller of the filing system and his representative, if any;

(2) the categories of personal data processed;

(3) the purposes of the data and the categories of body to whom they might be disclosed;

(4) the form of exercising the right of access and rectification.;

(5) any combinations of personal data processing;

(6) proposed transfers of data to third countries or regions.

2 – Any change in the information referred to in No. 1 shall be subject to the procedures provided for in Articles 21 and 22.

Article 25

Publicising of processing operations

1 – When personal data processing is not covered by a legal provision or statutory regulations with organizational nature, and must be authorised or notified, it shall be set down in a public authority register open to consultation by any person.

2 – The register shall contain the information listed in (1) to (4) and (9) of Article 23.
3 – A controller not subject to notification shall make available at least the information referred to in No. 1 of the previous article in an appropriate form to any person on request.
4 – This Article does not apply to processing whose sole purpose is the keeping of a register which according to laws or administrative regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest.
5 – All the opinions and authorisations drawn up or granted under this Act, particularly the authorisations provided for in No. 2 of Article 7 and No. 1 of Article 9, must be published by the public authority in its annual report.

CHAPTER VII
Codes of conduct

Article 26
Codes of conduct

The public authority shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the provisions in this Act, to enhance a great efficacy of self regulation, and to exercise and protect privacy pertained basic rights, taking account of the specific features of the various sectors.

Article 27
Submission of draft codes of conduct

1 – Professional associations and other bodies representing other categories of controllers which have drawn up draft codes of conduct shall be able to submit them to the public authority for registration.
2 – If the public authority considers the draft as in accordance with the laws and regulations in force in the area of personal data protection, a registration shall be made.
3 – The registration of the codes of conduct has the effect of a declaration of its lawfulness but does not have the nature of a legal provision or a statutory regulation.

CHAPTER VIII
Administrative and legal supervision

SECTION I
Administrative and legal supervision

Article 28
General principles

Without prejudice to the right to submit a complaint to the public authority, according to the law any individual may have recourse to administrative and legal means to guarantee compliance with legal provisions and statutory regulations in the area of personal data protection.

Article 29
Special legal supervision

1 – Appeals may be lodged directly to the Court of Final Appeal against decisions reached by a law court for the reason of violation of fundamental rights protected by this act. It shall be direct and limited to only the questions on violation against fundamental rights, and shall have an urgent nature.
2 – Without prejudice to the previous number, for administrative acts or simple facts of public powers, appeals may be lodged to the Administrative Court for reasons of violation of fundamental rights protected by this act. The appeal shall have an urgent nature.
3 – In compliance with the previous two numbers, Article 7 of the Codes of Civil Procedures shall apply to the duly adapted appeal procedure mentioned in the previous two numbers. It also applies to and supplements the duly adapted law of civil procedures and administrative procedures respectively.

SECTION II
Administrative offences

Article 30
Subsidiary legislation

The general system of administrative offences, adapted according to the following articles, is subsidiarily applicable to the offences provided for in this section.

Article 31

Compliance with duty omitted

Whenever the administrative offence arises from omitting a duty, application of the penalty and payment of the fine do not release the perpetrator from compliance with that duty, if it is still possible.

Article 32

Omission or inadequate compliance with obligations

1 – Bodies which negligently fail to comply with the obligation to notify the public authority of the processing of personal data referred to in No. 1 and No. 5 of Article 21, provide false information or comply with the obligation to notify without observing Article 23 or, having been notified by the public authority, continue to allow access to open data transmission networks to controllers who fail to comply with the provisions of this Act are committing an administrative offence punishable with the following fines:

(1) In the case of a natural person, a minimum of MOP2,000 and a maximum of MOP20,000;

(2) In the case of a legal person or a body without legal personality, a minimum of MOP10,000 and a maximum of MOP100,000.

2 – The fine shall be increased to double the maxima in the case of data subject to prior authorisation according to Article 22.

Article 33

Other administrative offences

1 – Bodies which fail to comply with obligations in Articles 5, 10, 11, 12, 13, 16, 17 and No. 3 of Article 25 are committing an administrative offence punishable with a minimum fine of MOP4,000 and a maximum of MOP40,000.

2 - In the case of failure to comply with the obligations in Articles 6, 7, 8, 9, 19 and 20, the administrative offence is punishable with a fine of MOP8,000 – MOP80,000.

Article 34

Concurrent offences

1 - If the same fact is simultaneously a crime and an administrative offence the agent shall always be punished by virtue of the crime.

2 – The penalties applied to concurrent administrative offences shall always be materially accumulated.

Article 35

Punishment of negligence and attempt

1 – Negligence shall always be punished in relation to the administrative offences provided for in Article 33.

2 - Any attempt to commit the administrative offences provided for in Articles 32 and 33 shall always be liable to punishment.

Article 36

Application of fines

1 – The public authority is responsible for the application of the fines provided for in this Act.

2 – The decision of the public authority shall be enforceable if it is not challenged within the statutory period.

SECTION III

Crimes

Article 37

Non-compliance with obligations relating to data protection

1 –Any person who intentionally:

(1) omits notification or the application for authorisation referred to in Articles 21 and 22;

(2) provides false information in the notification or in applications for authorisation for the processing of personal data or makes alterations in the latter which are not permitted by the legalisation instrument;

(3) misappropriates or uses personal data in a form incompatible with the purpose of the collection or with the legalisation instrument;

(4) promotes or carries out an illegal combination of personal data;

(5) fails to comply with the obligations provided for in this Act or in other data protection legislation when the time limit fixed by the public authority for complying with them has expired;

(6) continues to allow access to open data transmission networks to controllers who fail to comply with the provisions of this Act after notification by the public authority not to do so,

shall be liable to up to one year's imprisonment or a fine of up to 120 days.

2 – The penalty shall be increased to double the maxima in the case of the personal data referred to in Articles 7 and 8.

Article 38

Undue access

1 – Any person who without due authorisation gains access by any means to personal data prohibited to him shall be liable to up to one year's imprisonment or a fine of up to 120 days, if a more severe punishment is not to be enforced due to a specific law.

2 - The penalty shall be increased to double the maxima when access:

(1) is achieved by means of violating technical security rules;

(2) allows the agent or third parties to obtain knowledge of the personal data;

(3) provides the agent or third parties with a benefit or material advantage.

3 – In the case of No. 1 criminal proceedings are dependent upon a complaint.

Article 39

Invalidation or destruction of personal data

1 – Any person who without due authorisation erases, destroys, damages, deletes or changes personal data, making them unusable or affecting their capacity for use, shall be liable to up to two years' imprisonment or a fine of up to 240 days, if a more severe punishment is not to be enforced due to a specific law.

2 - The penalty shall be increased to double the maxima if the damage caused is particularly serious.

3 – If the agent acts with negligence as referred to in the previous two numbers the penalty in both cases shall be up to one year's imprisonment or a fine of up to 120 days.

Article 40

Qualified non-compliance

1 – Any person who after being notified to do so does not interrupt, cease or block the processing of personal data shall be subject to a penalty corresponding to the crime of qualified non-compliance.

2 – The same penalty shall apply to any person who after being notified:

(1) without just cause refuses to provide his cooperation specifically required by the public authority;

(2) does not erase or totally or partially destroy the personal data;

(3) does not destroy the personal data after the period for keeping them provided for in Article 5 has elapsed.

Article 41

Violation of the duty of secrecy

1 – Any person bound by professional secrecy according to the law who without just cause and without due consent reveals or discloses personal data, totally or in part, shall be liable to up to two years' imprisonment or a fine of up to 240 days, if a more severe punishment is not to be enforced due to a specific law.

2 - The penalty shall be increased by half the maxima if the agent:

(1) is a civil servant or equivalent, according to penal law;

(2) acts with the intention of obtaining a material advantage or other unlawful gain;

(3) adversely affects the reputation, honour and esteem or the privacy of another person.

3 – A person guilty of negligence shall be liable to up to six months' imprisonment or a fine of up to 120 days.

4 – Other than the cases provided for in No. 2, criminal proceedings are dependent upon a complaint.

Article 42

Punishment of attempt

Any attempt to commit the crimes provided for in this Section shall always be liable to punishment.

SECTION IV

Additional penalty

Article 43

Additional penalty

The following may be ordered in addition to the fines and penalties provided for in Sections II and III in this Chapter when applied:

(1) temporary or permanent prohibition of processing, blocking, erasure or total or partial destruction of data;

(2) publication of the judgement;

(3) public warning or censure of the controller by the public authority.

Article 44

Publication of judgement

1 – The judgement shall be published at the expense of the person judged in the periodicals with the largest circulation published, one in Chinese and one in Portuguese, and by means of affixing a notice for a period of no less than 30 days.

2 – Publication shall be done by means of a summary containing information on the offence and the penalties applied and the identification of the agent.

CHAPTER IX
Final provisions

Article 45

Transitional provision

1 – The processing of data held in manual filing systems on the date of the entry into force of this Act shall be brought into conformity with Articles 7, 8, 10 and 11 within two years.

2 – At his request the data subject may in any event, in particular when exercising the right of access, obtain the rectification, erasure or blocking of incomplete or inaccurate data or data kept in a manner incompatible with the legitimate purposes of the controller.

3 - The public authority may provide that the data held in manual filing systems and kept solely for the purposes of historical research need not be brought into conformity with Articles 7, 8 and 9, provided they are in no case reused for a different purpose.

Article 46

Entry into force

This Act comes into force on the 180th day following its publication.

Approved on 4 August 2005.

The President of the *Legislative Council, Susana Chou.*

Signed on 10 August 2005.

Hereby published.

The Chief Executive, HO HAU WAH.