Asia-Pacific
Economic Cooperation

2010/SOM3/ECSG/DPS/011
Agenda Item: VIIb

IAP – Malaysia

Purpose: Information
Submitted by: Malaysia

JAPAN 2010

Data Privacy Subgroup Meeting
Sendai, Japan
17 September 2010

Asia-Pacific Economic Cooperation

Information Privacy Individual Action Plan

Malaysia (2010)

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
A	Is privacy a constitutionally protected right in your economy?	No	Nil	Nil	Nil
B	If not, what other available legislation deals with privacy or confidentiality of personal information.	Malaysia on 4 May 2010 enacted the Personal Data Protection Act 2010. a) **PDP Act 2010** -	**a) Subsection 5(2)**	**Upon conviction** - i)fine not exceeding RM300, 000 ;	Enacted 10 June 2010

[1] *Note here the legislation, rule, code, framework or other privacy protection scheme. Where possible please provide the URL for the website where the legislation or arrangement is available.*

[2] *Insert the full text or summary of the provisions of your privacy protection scheme(s) that correspond to the APEC Privacy Principles identified in the column titled "APEC Principle/ Commentary".*

[3] *Sanctions should include the nature of the remedies available, the means by which they are obtained, and by whom (for example, government, local law enforcement, private right of action, etc.).*

[4] *Identify areas where the practice and the intent of the principle need further consideration; and identify the status of the economies' practice, for example enacted, introduced, draft. If your legislation, rule, code, framework or other privacy protection scheme is at the drafting or proposal stage and has not yet been enacted or implemented, please indicate here and provide any other useful comments."*

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
		i) regulates the processing of personal data of an individual in commercial transactions ii) safeguards the individual's privacy interests and prevent any abuse of personal data in the possession by the data user	(Non -adherence 7 Principles of data protection) **<u>PDP Act 2010 Subsection 5(1) PDP Principles</u>** **The processing of personal data by a data user shall be in compliance with the following PDP Principles;** **a)General** **b)Notice & Disclosure** **c)Disclosure** **d)Security** **e)Retention** **f)Data Integrity and** **g) Access** **b) <u>Subsection 16(4)</u>** (Processing without certificate of registration) **A person who belongs to the class of data users as specified in the order made under subsection 14(1) and who processes personal data without a certification of registration issued in pursuance of paragraph 16(1)(*a*) commits an offence and shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to**	or ii) imprisonment not exceeding 2 years ; or iii) both **<u>Upon conviction</u>** - i)fine not exceeding RM500, 000 ; or ii) imprisonment not exceeding 3 years ; or iii) both	

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			imprisonment for a term not exceeding three years or to both.		
			c) Subsection 18(4) (Continued processing after revocation of registration) **A data user whose registration has been revoked under this section (18) and who continues to process personal data thereaftercommits an offence and shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both.**	**Upon conviction** - i)fine not exceeding RM500, 000 ; or ii) imprisonment not exceeding 3 year ; or iii) both	
		b) **Banking and Financial Institutions Act 1989 – to safeguard** the confidentiality of personal and financial information of customers c) **Communications and Multimedia Act 1998** d) **Computer Crimes Act 1997** **(For (b), (c) and (d), please see Annexes)**	**d)Paragraph 23(2)(*d*)** (Non-compliance Code of practice) **The data user forum shall, in preparing a code of practice considers matters , including that the code of practice, … offers an adequate level of protection for the personal data of the data subjects concerned.**	**Upon conviction** –(Section 29) i)fine not exceeding RM100, 000 ; or ii) imprisonment not exceeding 1 year ; or iii) both	

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			e) <u>Subsection 40(1)</u> (Processing of sensitive data) **Subject to subsection (2) and section 5, a data user shall not process any sensitive personal data of a data subject except in accordance with the following conditions : among them –** **i)with the explicit consent of data subject;** **ii) fulfillment of legal obligations;** **iii) protection of vital interests of data subject or other person;** **iv) for medical purposes;** **v) administration of justice;** **vi) exercise of any functions conferred on any person by or under any written law** **f) <u>Subsection 43(1)</u>** (Direct marketing) **A data subject may, at any time at the end of any time by notice in writing to a data user at the end of such period as is reasonable to cease or not to**	**<u>Upon conviction</u>** - i)fine not exceeding RM200, 000 ; or ii) imprisonment not exceeding 2 years ; or iii) both **<u>Upon conviction</u>** - i)fine not exceeding RM200, 000 ; or ii) imprisonment not exceeding 2 years ; or iii) both	

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			begin processing his personal data for purposes of direct marketing. **g) <u>Subsection 129(1)</u>** (Transfer of personal data outside Malaysia) A data user shall not transfer any personal data of a data subject outside Malaysia unless to such place as specified by the Minister.	**<u>Upon conviction</u>** - i)fine not exceeding RM300, 000 ; or ii) imprisonment not exceeding 2 years ; or iii) both	
1	***I Preventing Harm*** **(Ref. Para. 14)** Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information	**a) <u>Personal Data Protection Act 2010</u>** **b) <u>Personal Data Protection Act 2010</u>**	**<u>a)Subsection 5(1)</u>** (Non - adherence to 7 Principles of data protection) **<u>1.PDP Act 2010 Subsection 5(1) PDP Principles</u>** **The processing of personal data by a data user shall be in compliance with the following PDP Principles;** **a)General** **b)Notice & Disclosure** **c)Disclosure** **d)Security** **e)Retention** **f)Data Integrity and** **g) Access** **b) <u>Subsection 42(1)</u>** (Right to prevent processing likely to cause damage or distress)	**<u>Upon conviction</u>** –Subsection 5(2) i)fine not exceeding RM300, 000 ; or ii) imprisonment not exceeding 2 years ; or iii) both	Enacted on 4 May 2010

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
			b)Subsection 42(1) **(Right to prevent processing likely to cause damage or distress)** **Subject to certain conditions in subsection (2), a data subject may at any time by notice in writing to a data user, require the data user at the end of such period as is reasonable in the circumstances, to –** **a)cease the processing of or processing for a specified purpose or in a specified manner; or** **b) not begin the processing of or processing for a specified purpose or in a specified manner,** **any personal data in respect of which he is the data subject if based on the reasons to be stated by him -** **A)…is causing or is likely to cause substantial damage or substantial distress to him or to another person; or** **B) the damage or distress is or would be unwarranted.**	**Upon conviction** –(Subsection 42(6) i)fine not exceeding RM200, 000 ; or ii) imprisonment not exceeding 2 years ; or iii) both	

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
2	***II Notice*** **(Ref. Para. 15-17)** Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include:	**a) <u>Personal Data Protection Act 2010</u>**	**<u>Subsection 7(1)</u>**	**<u>Upon conviction</u>** –[Subsection 5(2)] i)fine not exceeding RM300, 000 ; or ii) imprisonment not exceeding 2 years ; or iii) both	
	a)the fact that personal information is being collected;	**<u>Personal Data Protection Act 2010</u>**	a) Para. 7(1)(a) **<u>Paragraph 7(1)(</u>**a) A data user shall by written notice inform a data subject **- that personal <u>data of the data subject is being processed</u>**	same as above	
	b) the purposes for which personal information is collected;	**<u>Personal Data Protection Act 2010</u>**	b) Para. 7(1)(b) **<u>b)Paragraph 7(1)(b)</u>** **the <u>purposes for which the personal data is being or to be collected</u> and further processed**	same as above	
	c)the types of persons or organizations to whom personal information might	**<u>Personal Data Protection Act 2010</u>**	c) Para. 7(1)(e) **<u>c)Paragraph 7(1)(e)-</u>**	same as above	

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	be disclosed;		**of the <u>class of third parties to whom the data user discloses or may disclose</u> the personal data**		
	d)the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information;	**<u>Personal Data Protection Act 2010</u>**	d)Para. 7(1)(d) **<u>d)Paragraph 7(1)(d)</u>** **of the data subject's right to request access to … and <u>how to contact the data user with any inquiries and complaints</u> in respect of personal data.**	same as above	
	e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.	**<u>Personal Data Protection Act 2010</u>**	e) Para. 7(1)(f) **<u>Paragraph 7(1)(f)</u>** **<u>of the choices and means the data user offers the data subject for limiting the processing of personal data,</u> including personal data relating to other persons who may be identified from that personal data**	same as above	
	f)All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice	**<u>Personal Data Protection Act 2010</u>**	f)Paras. 7(2)(a),(b)(c [i]) **<u>f)Paragraphs 7(2)(a), (b) (c [i])</u>** **<u>The notice shall be given as practicable by the data user -</u>**	same as above	

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	should be provided as soon after as is practicable. It may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information.	 Nil	**a) When the data subject is first asked by the data user to provide his personal data ;** **b) When the data user first collects the personal data of the data subject;** **c) In any other case, before, the data user -** **i)Uses the personal data of the data subject for a purpose other than the purpose for which the personal data is collected** Nil	 Nil	
3	***III Collection Limitation*** **(Ref. Para. 18)** The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where	**<u>Personal Data Protection Act 2010</u>**	a) Para. 6(3)(b) (relevant to the purposes of collection) a)**<u>Para. 6(3)(b)</u>** (relevant to the purposes of collection)	**<u>Upon conviction</u>** – i)fine not exceeding RM300, 000 ; or ii) imprisonment not exceeding 2 years ; or iii) both	Nil

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	appropriate, with notice to, or consent of, the individual concerned.		**Personal data shall not be processed unless the processing of the personal data is necessary <u>for or directly related to that purpose</u>** b) Para. 7(1)(b) **<u>b)Para. 7(1)(b)</u> (with notice to) <u>A data user</u> shall b<u>y written notice inform a data subject</u> the purposes for which the personal data is being or is to be collected and further processed.** c) Para. 6(1)(a) (with consent) **A data user shall not in the case of personal data other than sensitive personal data , process data about a data subject <u>unless the data subject has given his consent</u> to the processing of the personal data**	**Sanction applicable for all 3 paragraphs mentioned here**	
4	***IV Use of Personal Information*** **(Ref. Para. 19)** Personal information	**<u>Personal Data Protection Act</u>**	a) Para. 6(1)(a)		

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	collected should be used only to fulfill the purposes of collection and other compatible or related purposes except: a)with the consent of the individual whose personal information is collected; b) when necessary to provide a service or product requested by the individual; or, c)by the authority of law	**2010** **Personal Data Protection Act 2010** **Personal Data Protection Act**	**a)Para. 6(1)(a)** **(with consent)** **A data user shall not in the case of personal data other than sensitive personal data , process data about a data subject unless the data subject has given his consent to the processing of the personal data** b) Paras. 6(2)(a),(b) **b) Paras. 6(2)(a) & (b)** **Notwithstanding paragraph (1)(a), a data user may process personal data about a data subject if the processing is necessary –** **a)for the performance of a contract to which the data subject is a party ;** **b) for the taking of steps at the request of the data subject with a view to entering into a contract**; c) Paras. 6(2)(d),(e) & (f)	**Upon conviction** - i)fine not exceeding RM300, 000 ; or ii) imprisonment not exceeding 2 years ; or iii) both **Same as above**	Nil Nil

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	and other legal instruments, proclamations and pronouncements of legal effect.	**2010**	**c)Paras. 6(2)(d),(e) & (f)** **d)in order to protect the vital interests of the data subject;** **e)for the administration of justice; or** **f)for the exercise of any functions conferred on any person by or under any law.**	**Same as above**	Nil
5	*V Choice* (Ref. Para. 20) Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.	**Personal Data Protection Act 2010** **Nil**	Subsection 7(3) **Subsection 7(3)** **A notice under shall be in the national and English languages , and the individual shall be provided with a clear and readily accessible means to exercise his choice , where necessary , in the national and English languages.** Nil	**Upon conviction** - i)fine not exceeding RM300, 000 ; or ii) imprisonment not exceeding 2 years ; or iii) both	Nil

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
6	***VI Integrity of Personal Information*** **(Ref. Para. 21)** Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.	**Personal Data Protection Act 2010**	**Section 11** **A data user shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed.**	**Upon conviction** - i)fine not exceeding RM300, 000 ; or ii) imprisonment not exceeding 2 years ; or iii) both	Nil
7	***VII Security Safeguards*** **(Ref. Para. 22)** Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the	**Personal Data Protection Act 2010**	**Section 9** **A data user shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction by having regard -** **a)to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or**	**Upon conviction** - i)fine not exceeding RM300, 000 ; or ii) imprisonment not exceeding 2 years ; or iii) both	Nil

	APEC Principle / Commentary	Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [1]	Provision[2]	Sanction[3]	Results/ Status[4]
	sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.		**destruction;** **b)to the place or location where the personal data is stored;** **c)to any security measures incorporated into any equipment in which the personal data is stored;** **d)to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and** **e)to the measures taken for ensuring the secure transfer of the personal data.**		

8	***VIII Access and Correction*** **(Ref. Para. 23-25)** Individuals should be able to:	**Personal Data Protection Act 2010**			

	a)obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them; b) have communicated to them, after having provided sufficient proof of their identity, personal information about them; i. within a reasonable time; ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; iv. in a form that is		Subsection 30(1) (Not later than 21 days) **<u>Subsection 30(1)</u>** **An individual is entitled to be informed by the data user whether personal data of which that individual is a data subject is being processed by or on behalf of the data user** Subsection 31(1) **<u>i)Subsection 31(1)</u>** .. ..**a data user shall comply with a data access request not later than twenty-one days from the date of receipt of the data access request** ii) Para. 30(2)(a) **A requestor may, upon payment of a prescribed fee, make a data access request in writing to the data user for information of the data subject's personal data that is being processed by or on behalf o f the personal data** iii) Nil iv) Para. 30(2)(b)	Nil Nil Nil Nil Nil	Nil Nil Nil Nil Nil

	generally understandable; and, c)challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.		**<u>iv. Paragraph 30(2)(b)</u>** **A requestor may, upon payment of a prescribed fee, make a data access request in writing to have communicated to him a copy of the personal data in an intelligible form.** c)Subsection 34(1) **<u>Subsection 34(1)</u>** **<u>Where –</u>** **a)a copy of the personal data has been supplied by the data user in compliance with the data access request … and the requestor considers that the personal data is inaccurate, incomplete , misleading or not up-to-date; or** **b)the data subject knows that his personal data being held by the data user is inaccurate, incomplete , misleading or not up-to-date ,** **the requestor or data subject , as the case may be, may make a data correction request in writing to the data user that the data user makes the necessary correction to the personal data.**	Nil	Nil

			Para. 35(1)(a) (Not later than 21 days) **<u>Paragraph 35(1)(a)</u>** **<u>(Not later than 21 days)</u>** **<u>Compliance with data correction request</u>** **… where a data user is satisfied that the personal data to which a data request relates is inaccurate, incomplete , misleading or not up-to-date, he shall, not later than twenty-one days from the date of receipt of the data correction request -** **a)make the necessary correction to the personal data;** **b)supply the requestor with a copy o f the personal data so corrected.**	Nil	Nil
	Such access and opportunity for correction should be provided except where: (i) the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in		i)Para. 32(1)(c) **<u>i)Paragraph. 32(1)(c)</u>** **A data user may refuse to comply with the data access request if the burden or expense of providing access is**	Nil	

	question;		**disproportionate to the risks to the data subject's privacy in relation to the personal data in the case in question**		
	(ii) the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or		ii)Paras. 32(1)(f),(g) & (h) **<u>ii) Paragraphs. 32(1)(f),(g) & (h)</u>** **A data user may refuse to comply with the data access request if -** **f)<u>providing access would constitute a violation of an order of a court;</u>** **<u>g)providing access would disclose confidential commercial information ; or</u>** **<u>h)such access to personal data is regulated by another law</u>**	Nil	
	(iii) the information privacy of persons other than the individual would be violated.		iii)Para. 32(1)(d) **<u>iii) Paragraph 32(1)(d)</u>** **A data user may refuse to comply with the data access request if the data user cannot comply with the data access <u>request without disclosing personal data relating to another person who can be identified from that information</u>**	Nil	

	If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial.		**<u>unless -</u>** **i)that other individual has consented to the disclosure of the information to the requestor** **<u>a)Paragraph. 31(2)(a)</u>** **A data user who is unable to comply with a data access request within the period specified (i.e. not later than 21 days from the date of receipt of the request) shall before the expiration of that period by notice in writing inform the requestor that he is unable to comply with the data access request within such period and the reasons why he is unable to do so.** **<u>b)Paragraph 33(a)</u>** **Where a data user who pursuant to certain conditions refuses to comply with the data access request , he shall not later than twenty-one days from the date from the date of receipt of the data access request , by notice in writing, inform the requestor of the refusal and the reasons for the refusal.**		

			c)Subsection 35(2) **A data user who is unable to comply with a data correction request within the period specified (i.e. not later than 21 days from the date of receipt of the request) shall before the expiration of that period by notice in writing inform the requestor that he is unable to comply with the data correction request within such period and the reasons why he is unable to do**		
9	***IX Accountability*** **(Ref. Para. 26)** A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the **consent of the individual** or exercise due diligence **and take reasonable steps to ensure that the recipient**	P**ersonal Data Protection Act 2010**	**Paragraph 129(3)(a)** (Consent of individual) **Paragraph 129(3)** (Consent of individual) **Notwithstanding subsection (1), a data user may transfer any personal data to a place outside Malaysia if the data subject has given his consent to the transfer** **Paragraph 129(2)** **For the purpose of subsection (1) , the Minister may specify**	**Subsection 129(5)** **Upon conviction** - i)fine not exceeding RM300, 000 ; or ii) imprisonment not exceeding 2 years ; or iii) both Applicable to all the paragraphs mentioned here	Nil

	person or organization will protect the information consistently with these Principles. .		**any place outside Malaysia if –** **a)there is in that place in force any law which is substantially similar to this Act, or serves the same purpose as this Act ; or** **b)that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by this Act.** **Paragraph 129(3)(f)** (Adequate protection by recipient) **Notwithstanding subsection (1), a data user may transfer any personal data to a place outside Malaysia if the data user has taken all reasonable precautions and exercised all diligence to ensure that the personal data will not in that place be processed an any manner which, if that place is Malaysia, would be a contravention of this Act. Paragraph 129(3)(f)**		
C	Network point of contact arrangements[5]	Contact details will be made available to APEC members through the APEC Secretariat.			Nil

[5] *Please provide contact details such as name and/or title, address, telephone and email contacts. This information will not be published but will be made available to economies.*

-- // --

ANNEXES

INFORMATION PRIVACY INDIVIDUAL ACTION PLAN
MALAYSIA (2010)

OTHER AVAILABLE LEGISLATION DEALS WITH PRIVACY
OR CONFIDENTIALITY OF PERSONAL INFORMATION.

1. Banking and Financial Institutions Act 1989
2. Communications and Multimedia Act 1998
3. Computer Crimes Act 1997

BANKING AND FINANCIAL INSTITUTIONS ACT 1989 (BAFIA)

The BAFIA 1989 Act provides for the licensing and regulation of institutions carrying on banking, finance company, merchant banking, discount house and money-broking businesses, for the regulation of institutions carrying on certain other financial businesses.

Under the Act, there are 2 provisions to protect the confidentiality of personal information of individuals and the privacy of particular customers. The provisions are specified in Sections 96 and 97 (1) as follows-

a) - **Section 96 PROVIDES for Restriction on inquiring specifically into affairs of particular customer which states that -**

96. Except as provided in section 43 (2), and without prejudice to the powers of inspection, examination, investigation or inquiry conferred on the Bank or on an investigating officer under this Act, nothing in this Act shall—

(a) authorise the Minister to direct the Bank; or

(b) authorise the Bank,

to inquire specifically into the affairs of any individual customer of any licensed institution.

Section 43(2)

(2) Notwithstanding the provisions of sections 96 and 97, the Bank may require—

any class or category of licensed institutions, other than a licensed discount house or a licensed money-broker, to submit a statement showing such credit information relating to their customers as is required for the purposes of the credit bureau established under section 30 (1) (*mmm*) of the Central Bank of Malaysia Act 1958; and

b) Section 97 PROVIDES for Secrecy which states that –

97. (1) No director or officer of any licensed institution or of any external bureau established, or any agent appointed, by the licensed institution to undertake any part of its business, whether during his tenure of office, or during his employment, or thereafter, and no person who for any reason, has by any means access to any record, book, register, correspondence, or other document whatsoever, or material, relating to the affairs or, in particular, the account, of any particular customer of the institution, shall give, produce, divulge, reveal, publish or otherwise disclose, to any person, or make a record for any person, of any information or document whatsoever relating to the affairs or account of such customer. *Act A954.*

(2) This section shall not apply to any information or document which at the time of the

disclosure is, or has already been made, lawfully available to the public from any source other than the licensed institution, or to any information which is in the form of a summary or collection of information set out in such manner as does not enable information relating to any particular licensed institution or any particular customer of the licensed institution to be ascertained from it.

(3) No person who has any information or document which to his knowledge has been disclosed in contravention of subsection (1) shall in any manner howsoever disclose the same to any other person.

HOWEVER there are provisions that allow disclosure of any information or document under certain circumstances as in Sections 98 , 98A and 99 –

1) **Section 98 – allows disclosure for facilitating performance of functions by Bank**
2) **Section 98A - allows disclosure for facilitating performance of functions by Malaysia Deposit Insurance Corporation**
3) **Section 99 - allows for other permitted disclosures such as :-**

(a) which the customer, or his personal representative, has given permission in writing to disclose;

(b) in a case where the customer is declared bankrupt, or, if the customer is a corporation, the corporation is being or has been wound up, in Malaysia or in any economy, territory or place outside Malaysia;

(c) where the information is required by a party to a *bona fide* commercial transaction, or to a prospective *bona fide* commercial transaction, to which the customer is also a party, to assess the creditworthiness of the customer relating to such transaction, provided that the information required is of a general nature and does not enable the details of the customer's account or affairs to be ascertained;

(d) for the purposes of any criminal proceedings or in respect of any civil proceedings— *Act A954.*

(i) between a licensed institution and its customer or his guarantor relating to the customer's transaction with the institution; or

(ii) between the licensed institution and two or more parties making adverse claims to money in a customer's account where the licensed institution seeks relief by way of interpleader;

(e) where the licensed institution has been served a garnishee order attaching monies in the account of the customer;

(f) to an external bureau established, or to an agent appointed, by the licensed institution with the prior written consent of the Bank; *Act A954.*

(g) where such disclosure is required or authorised under any other provision of this Act;

(h) where such disclosure is authorised under any Federal law to be made to a police officer investigating into any offence under such law and such disclosure to the police officer being, in any case, limited to the accounts and affairs of the person suspected of the offence; or *Act A954.*

(i) where such disclosure is authorised in writing by the Bank. *Act A954.*

(2) In any civil proceedings under subsection (1) *(b)* or *(d)* where any information or document is likely to be disclosed in relation to a customer's account, such proceedings may, if the court, of its own motion, or on the application of a party to the proceedings, so orders, be held *in camera* and in such case, the information or document shall be secret as between the court and the parties thereto, and no such party shall disclose such information or document to any other person.

(3) Unless the court otherwise orders, no person shall publish the name, address or photograph of any parties to such civil proceedings as are referred to in subsection (2), or any information likely to lead to the identification of the parties thereto, either during the currency of the proceedings or at any time after they have been concluded.
PENALTY - RM3 MILLION OR 3 YEARS IMPRISONMENT

Communications and Multimedia Act 1998 (CMA Act)

Sections 233 (1), 234 (1) (b) (c) and (2) of the CMA 1998 also provide another means to safeguard the privacy of an individual .

Subsection 233(1) - A person who –

a) By means of any network facilities or network service or applications service knowingly -

(i) makes, creates or solicits; and

(ii) initiates the transmission of ,

any comment, request , suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person; or

b) initiates a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address,

commits an offence .

Penalty - **Subsection 233(3)**
i) Fine not exceeding RM50,000 ; or
ii) Imprisonment not exceeding 1 year;
iii)both

Shall also be fined RM1000 for every day during which the offence is continued after conviction

Section 234 (1) - A person who, without lawful authority under this Act or any written law -

b) discloses, or attempts to disclose , to any other person the contents of any communications, knowing or having reason to believe that the information was obtained through the interception of any communications in contravention of this section; or

c) uses, or attempts to use, the contents of any communications, knowing or having reason to believe that the information was obtained through the interception of any communications in contravention of this section,

commits an offence

Penalty - i) Fine not exceeding RM50,000 ; or
ii) Imprisonment not exceeding 1 year;
iii)both

Subsection 234 (2) A person authorised under this Act who intentionally discloses, or attempts to disclose , to any other person the contents of any communications, intercepted by means authorised by this Act –

(a) knowing or having reason to believe that the information was obtained through the interception of such communications in connection with a criminal investigation ;

(b) having obtained or received the information in connection with a criminal investigation ;,

commits an offence

Penalty – **Subsection 234 (3)**

i) Fine not exceeding RM50,000 ; or
ii) Imprisonment not exceeding 1 year; or
iii) both

Computer Crimes Act 1997

Subsection 3 - Unauthorised access to computer material

Subsection 3(1) A person shall be guilty of an offence if –

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorized; and

(c) he knows at the time when he causes the computer to perform the function that that is the cause.

Subsection 3(2) The intent a person has to have to commit an offence under this section need not be directed at –

(a)any particular program or data;

(b)a program or data of any particular kind; or

(c) a program or data held in any particular computer.

Penalty (Subsection 3 (3) –

i) Fine not exceeding RM50,000 ; or

ii) Imprisonment not exceeding 1 year;

iii) both

General Consumer Code of Practice For Communications and Multimedia Industry October 2009 under the CMA 1998

The Ministry of Information, Communications and Culture through the Malaysian Communications and Multimedia Commission had made it mandatory for all Service Providers to comply with General Consumer Code of Practice For Communications and Multimedia Industry (October 2009) . Here all communication service providers are governed by a consumer code and must not disclose customers' personal information to other parties. As provided under the Communications and Multimedia Act 1998 , the Code and subcodes developed bind the following –

(a) all licensed service providers as far as their licensed activities are concerned;
(b) all non-licensed service providers who are members of the Consumer Forum.

The Consumer Forum will administer all codes developed by the Forum

Part 2 of the General Consumer Code sets out the responsibility of a service provider in the protection of consumer information of the communications and multimedia services in Malaysia. Generally, a service provider may collect and keep the personal information of their customers for record purposes to be used for tracking practices. However the service providers

cannot share their customer's personal information with nor transfer them to other parties without the prior approval from the customers concerned.

Service providers must also take appropriate measures to provide adequate security, and respect customers' preferences regarding unsolicited mail and telephone calls. Service providers must be open, transparent , and meet generally accepted fair information principles, including providing notice as to what personal information they collect, use and disclose; the choices consumers have with regard to the collection, use and disclosure of that information; the access consumers have to the information; he security measures taken to protect the information; and the enforcement and redress mechanisms that are in place to remedy any violation of these.

REDRESSAL OF BREACHES/VIOLATIONS:

1. **Sanctions Subsection 6.9**

   The types of sanction that can be imposed are –

   (a) issuance of a caution notice ;
   (b) issuance of a warning notice

2. **Referral to the Communications and Multimedia Commission**

   Subsection 6.10

   In the case of continued breaches of Registered codes, the Forum will use its discretion as to whether to refer a matter to the MCMC for consideration, The Forum will use the full mechanisms of this complaint handling and sanction process before referral to the MCMC.

The Forum will monitor the adoption of sanctions, rectification and appeals.

3. **Compensation**

   General Principles of Compensation

   Subsection 6.18

   Service providers must offer compensation to customers in cases of a breach of the Consumer Code and any relevant mandatory standards
   that have been issued and will be issued from time to time by MCMC regarding a matter dealt with in this Code or the said Mandatory Standard. It is accepted that compensation is not meant to penalize Service Providers not to unjustly enrich customers. As far as possible customers are to be placed in the same positions they were prior to the breach.

   Compensation packages may be in monetary or non-monetary form, and may take the form of refund, rebates, waivers, free activation, etc. It is also recognized that compensation packages differs from industry to industry and specific compensatory packages relevant to industry may be further elaborated in the sub-codes. Compensation is not intended to and shall not amount to a penalty on service providers whether in the form of special or consequential losses or damages or
   otherwise.