THE MALAYSIAN
PERSONAL DATA PROTECTION ACT:
WHAT IT MEANS FOR DATA USERS

Professor Abu Bakar Munir
Faculty of Law, University of Malaya
Former Adviser to the Government of Malaysia
on Data Protection

MSC MALAYSIA
PERSONAL DATA PROTECTION CONFERENCE
The Royale Chulan Hotel, Kuala Lumpur
19 July 2010
I am often accused of interfering in the private lives of citizens.
Yet, if I did not, had I not done that, we wouldn't be here today.
We decide what is right; never mind what the people think. That's another problem.

~Lee Kwan Yew 1986 ~
Great deal of information is already being gathered about each of us, by private companies as well as government agencies, and we often have no idea how it is used or whether it is accurate.

~ Bill Gates, 1996 ~
Outline

- International Instruments
- Data Protection - World Tour
- Malaysia: Data Protection Journey
- The PDPA Basic
- Enough is Enough
- What’s Now?
- Concluding Remarks
International Instruments

- OECD Guidelines 1980
- Council of Europe Convention 1981
- European Directive 1995
- APEC Privacy Framework 2004
- Madrid Resolution 2009
Data Protection - World Tour

Data Protection Laws Around the World

- Blue: Comprehensive Data Protection Law Enacted
- Red: Pending Effort to Enact Law
- White: No Law
- Comprehensive Legislation
- Legislation + Self-Regulatory
- Self-Regulatory
- Doing Nothing
Comprehensive Legislation

- All EU countries, including the 10 new member states (Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia and Slovenia)
- Japan, Korea, New Zealand, Australia, Hong Kong, Macao, Taiwan, Thailand, Philippines
- Chile, Argentina, Brazil, Mexico
- In Middle East, only Israel
- Indonesia and China are working on a comprehensive data protection law.
- Legislation + Self-Regulatory
  - USA – Privacy Act 1974 + 12 federal sectoral based legislation + State Laws + Safe Harbour

- Self-Regulatory
  - Singapore
Doing Nothing so far

- Brunei
- Vietnam
- Laos
- Cambodia
- Many more
Malaysia: Data Protection Journey

- 2000: First draft
- Available to public for comment
- 2002: Published a book on Privacy and Data Protection
- 2007: CTOS
- 2007: New draft
- 2009: First reading
- 2010: 5 April-Second & third reading
- 2010: 4 May-Dewan Negara
- 2010: 2 June-Royal Assent was granted
- 2010: 10 June-Gazetted
Personal data protection commission to function from next January

KUALA LUMPUR: A commission under the Personal Data Protection Act 2009 will be created by January next year, said Information, Communication and Culture Minister Datuk Seri Dr Rais Yatim.

He said the secretary-general of the ministry, Datuk Wira Kamaruddin Siaraf, was now discussing with the Public Service Department (PSD) on the manpower needs, emoluments and other service requirements for the commission.

"The commission has already been created in terms of legislation, it's just that we need to cooperate with the PSD and accept the location of the building, which we are working on now.

"I think it's not later than January next year, but probably by the end of the year, we can resolve the size of the manpower required. We are also planning the logistics for the new department," he told reporters after presenting the 2009 Excellent Service Awards to ministry staff, here Tuesday.

Rais said that with the existence of the commission, the number of agencies and departments under the ministry had increased to 19.

He said the commission was closely linked to the Malaysian Communications and Multimedia Commission (MCMC) as it applied computer forensic knowledge.

"In addition, the commissioner is not just anybody. He has to be trained in interrogations, cross-examinations in court proceedings and others," he said.
The PDPA Basic

- Scope and Application
- Data Protection Principles
- Exemptions
- Rights of Data Subject
- Criminal Offences
- Enforcement and Compliance Mechanisms
Scope and Application

- Federal & States Govts
- Non-Commercial Transactions
- Credit Reference Agencies
- Personal, Family & Household Affairs
- Data Processed Outside Malaysia
Personal Data

- Data relates directly or indirectly to a data subject
- Who is identified or identifiable from that information and other information in the possession of data user
Automatic and Manual Data

- Processed wholly or partly by means of equipment operating automatically
- Relevant filing system
Cont...

Processing

☐ collecting
☐ recording
☐ holding
☐ storing
☐ organising
☐ etc.
Data Users
- A person who either alone or jointly or in common with other persons processes or authorizes the processing of any personal data or has control over personal data, but does not include a data processor

Data Subject
- An individual who is the subject of the personal data
Data Protection Principles

- GENERAL PRINCIPLE
- NOTICE & CHOICE PRINCIPLE
- ACCESS PRINCIPLE
- DISCLOSURE PRINCIPLE
- DATA INTEGRITY PRINCIPLE
- RETENTION PRINCIPLE
- SECURITY PRINCIPLE
Data Protection Principles

1. General Principle - Personal Data cannot be processed without the consent of data subject

☐ Exemptions

- for the performance of a contract to which the data subject is a party
- at the request of the data subject with a view to entering into a contract
- to protect the vital interest of the data subject
2. Notice and Choice Principle

A data user shall inform the data subject that;

☐ the personal data of the data subject is being processed and provide a description of the personal data

☐ the purposes of the collection

☐ the right of the data subject to request access
3. Disclosure Principle

No personal data shall, without the consent of the data subject, be disclosed for other purposes.

4. Retention Principle

Personal data processed for any purpose shall not be kept longer than is necessary for the fulfillment of that purpose.
5. **Data Integrity Principle**

Data user shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date.

6. **Access Principle**

A data subject shall be given access to his personal data and shall be able to correct that personal data if it is inaccurate, incomplete, misleading or not up-to-date.
7. Security Principle

A data user shall take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.
Exemptions

- Prevention or detection of crime
- Apprehension or prosecution of offenders
- Assessment or collection of tax or duty
- Physical or mental health
- Statistics or research
- Court order or judgement
- Regulatory functions
- Journalistic, literary or artistic purposes

- Personal, family or household affairs
Rights of Data Subject

RIGHT TO BE INFORMED

RIGHT TO CORRECT

RIGHT TO WITHDRAW CONSENT

RIGHT TO ACCESS

RIGHT TO PREVENT PROCESSING LIKELY TO CAUSE DAMAGE OR DISTRESS

RIGHT TO PREVENT PROCESSING FOR DIRECT MARKETING PURPOSES
Rights of Data Subject

1. Right of Access to Personal Data

An individual is entitled to be informed by the data user whether the personal data of which that individual is the data subject is being processed:
- request in writing
- upon payment of a fee
- a data user should comply within a specified time period
2. Right to Correct Personal Data

Where a data user is satisfied that the personal data is inaccurate, incomplete, misleading or not up-to-date, he shall not later than twenty-one days;
- make the necessary correction
- supply the requestor with a copy of the personal data as corrected
3. Right to prevent processing likely to cause damage or distress

At any time, a data subject can require the data user to cease the processing of or not to begin the processing of the personal data if it causes or likely to cause substantial damage or distress.
4. Right to prevent processing for direct marketing purposes

A data subject may at any time require the data user to cease or not to begin processing the personal data for the purpose of direct marketing.

A data user who fails to comply with the notice commits an offence.
Criminal Offences

- SELLING DATA
- FAILURE TO REGISTER
- CONTRAVENE DATA PROTECTION PRINCIPLES
- UNLAWFUL COLLECTION
- PROCESSING AFTER REGISTRATION REVOKED
- TRANSFER DATA WITHOUT ADEQUATE PROTECTION
- FAILURE TO COMPLY WITH ENFORCEMENT NOTICE
- DISCLOSURE WITHOUT CONSENT
Some Criminal Offences

- Contravene any of the Data Protection Principles
- Failure to comply with the requirements of the Data Protection Commissioner in relation to the right to prevent processing that cause damage or distress
- Failure to comply with the requirements of the Data Protection Commissioner in relation to the right to prevent processing for direct marketing purposes
- Transfer of data to places outside Malaysia whenever there is no law in force to protect the personal data or there is no adequate level of protection.
- Collect, disclose or procures the disclosure of personal data without the consent of data user
- Failure to comply with the enforcement notice
If a body corporate commits an offence, any person who at the time of the commission of the offence was a director, chief executive officer, manager, secretary, etc, may be charged severally or jointly in the same proceeding. If the body corporate is found to have committed the offence, the officers are deemed to have committed the offence personally.
Enforcement and Compliance Mechanisms

- Data Protection Commissioner
- Advisory Committee
- Appeal Tribunal
- Codes of Practice
- Enforcement Notice
- Prosecution
- Revocation of Registration
Enough is Enough

Data sale racket

Your personal details can be bought for just 10 sen

By JOSEPH LOH and RASHVINJEET S. BEDI
sunday@thestar.com.my

KUALA LUMPUR: For a mere 10 sen, your personal data are being sold to unauthorised bodies. A list of 1,000 entries containing names, handphone numbers, type of credit card owned and issuing banks, and place of work costs only RM100.

If you regularly receive unsolicited sales calls, messages or e-mails, then in all likelihood, your data have been collected and sold to third parties.

With such baseline information in the hands of the unscrupulous, more particulars could easily be gathered and your identity stolen – for transactions and the purchase of goods or services without your knowledge.

A list obtained by Sunday Star linked individuals to credit cards although banks regard the leaking of information as a very serious offence.

Those caught for this offence could be subjected to punishment under Section 97 of the Banking and Financial Institutions Act.

Association of Banks in Malaysia executive director Chuah Mei Lin said that member banks treated customer information with the greatest of confidentiality and

The STAR headline 03 May 2009
EMAIL ADDRESS FOR SALE FROM RM 9.90 ONLY

Promote your Own Blog / Biz / Product to over 300 million active internet user daily!

mail us at

Lepak2u@yahoo.com

for more details n Our full profile reviews

TQ
Govt stops using CTOS

PUTRAJAYA: The cabinet decided on Wednesday that all government departments and agencies can no longer use services provided by credit reference company CTOS Sdn Bhd.

Second Finance Minister Tan Sri Nor Mohamad Yakin said this in response to a directive which takes immediate effect.

"A circular has been issued, that no government departments or agencies will use CTOS, period," he said when asked on the status of CTOS and the proposed Data Protection Bill.

He was speaking after presenting excellent service awards to 150 ministry staff yesterday.

Nor Mohamed also said a legislature will be introduced for private agencies that provide credit reference information.

"Currently, we don't have a mechanism and we want to [regulate] these agencies now," he said.

He said the government had a benchmark on quality and what type of people they should provide information to. So we want to bring them under this [regulatory] framework."

He added that while waiting for the draft of the Bill to be ready, the ministry, through Bank Negara, has informed the banks that they cannot use the services of CTOS "unless and until they have approval from their clients."

Asked why the banks do not depend on the service provided by Bank Negara's Central Credit Reference Information System (CCRIS), Nor Mohamed said the Ministry of Finance and Deputy Finance Minister Datin Awang Adek is looking into this. He said the task force has had two meetings with Bank Negara officials on the proposed Data Protection Bill, which is expected to be completed in December before being tabled in Parliament.

Financial institutions refer to information from credit reference agencies to help them determine the credit-worthiness of loan applicants. Other information to determine creditworthiness includes income verification, work history, and personal references.

In recent weeks, the company has come under the spotlight following allegations that some loan applicants were rejected as a result of its outdated information, and complaints about it divulging a person's credit information without his/her permission.

The Companies Commission of Malaysia then filed 85 charges against CTOS and three related companies for flouting regulations, such as failing to submit profit and loss statements and annual reports.

On Monday, the Association of Banks in Malaysia said it will get written consent from applicants before checking their information with CTOS.

Various parties have urged the government to set up a regulatory framework like the Data Protection Act to prevent abuse.
Jawatankuasa siasat sistem PTG diceroboh

Oleh NIZAM YATIM
dan JOHARI SYAWAL

18/3/2003

KUALA LUMPUR 14 Mac - Kementerian Sumber Asli dan Alam Sekitar yang menyendiri pencerobohan Sistem Pendaftaran Tanah Berkompuler berlaku di Pejabat Tanah dan Galian (PTG) beberapa negeri sedia menubuhkan sebuah jawatankuasa khas bagi menyiaskan dakwaan tersebut.

Setiausaha Parlimen kementerian berkenaan, Datuk Sazmi Miah berkata, pihaknya memang menyendiri kegiatan tersebut namun siasatan sebelum ini mendapat kejadian itu tidak melibatkan 'orang dalam'.

"Setakat ini tiada kaitan sama ada yang berkhidmat dengan Jabatan Ketua Pengarah Tanah dan Galian (JKPTG) di bawah kementerian atau PTG dikesan terlibat dalam kes itu."

"Jika polis mempunyai bukti terbaru, kementerian bersedia menubuhkan jawatankuasa khas bagi menyiaskan dakwaan ini di peringkat daerah kerana kita tidak bertolak ansur terhadap perbuatan sedemikian," katanya ketika dihubungi Utusan Malaysia di sini hari ini.


Menurut Ramli, modus operandi penceroboh tersebut adalah dengan mendakwa ge-ran tanah milik mereka hilang sebelum mendapatkan semula geran baru yang telah dipinda melalui bantuan 'orang dalam' sebelum menandatangani tanah itu pada harga tinggi.

Sazmi berkata, pemantauan pihaknya sebelum ini mendapat kegiatan jenis sehingga di PTG lebih tertumpu kepada pemalsuan kad pengenalan semasa memohon geran tanah gantian.

Lihat muka 2
Datuk sought over RM21mil land scam

BY LOURDES CHARLES

KUALA LUMPUR: A well-known property developer who is a Datuk is being sought by police for alleged involvement in a land scam worth RM21mil.

It is learnt that the City Police Commercial Crimes Department have arrested three people and are looking for at least five more, including the Datuk, who were alleged to have duped the KL Land Office into transferring ownerships of land to their name.

Sources said the City Police Commercial Crimes Department busted the syndicate's activities following a report lodged last month by the director of a company who owned the land.

They said the Datuk and his accomplices had duped the Land Office during the upgrading of its computerisation programme. (The Land Office had previously recorded the transactions manually and had only recently been fully computerised.)

They said the Datuk and his accomplices had mortgaged the land to an insurance company for more than RM10mil and were in the process of obtaining more money for the land when the police moved in.

The sources also said that the scam was exposed when the owner of the land, who is a company director, went to pay quit rent at the KL Land Office and was told that the quit rent had already been paid.

Upon further enquiries, the director was told by a land officer that he was not the owner of the land. The director then furnished proof to the Land Office and later lodged a report at the City Police Commercial Crimes Department.

A task force headed by City Commercial Crimes chief ACP Mohamad Arif and Deputy Supt Mohamad Shariff Wahid conducted a series of operations that led to the arrest of three suspects.

They have been remanded and are expected to be charged soon.

City Chief Police Officer Deputy Commissioner Datuk Mustafa Abdullah confirmed the report and the arrests.

"We have solved the case and are looking for several more suspects whose identity are known to us," he said.
Telco A

- Privacy policy of Telco A is not easy to locate.
- It does not appear on its website but available on the website of one of its products/services – IP Telephony
- “Personal information held by Telco A may include your name, date of birth, current address, telephone/mobile phone number, email address, credit cards details, occupation, user ID or password... as well as certain details about your personal interest.”
- “Telco A complies with and is registered under the data protection law in Malaysia and...”
Telco B

- “It takes the issue of privacy seriously.”
- It collects data such as name, identity card/passport number, postal address, date of birth and sex
- “The individually identifiable information may be used extensively within our company and our related and affiliated corporation.”
ISP A

“ISP A will endeavor to protect your data and privacy in using the services, which shall be based on ISP A’s confidentiality and privacy policy published on ISP A’s website.”

Privacy policy is not in the most accessible and easy to read manner.

The privacy policy is too brief and general.
Bank A

“Any information sent to Bank A Bhd through the use of this site will be deemed not to be confidential and be deemed to remain the property of Bank A Bhd who shall be free to use, copy, publish, reproduce, distribute and/or transmit all such information at Bank A Bhd’s absolute discretion for any purpose and...”
Bank B

“Your data maybe use by Bank B Bhd and/or its related companies for the purpose of researching, designing, launching, promoting, and marketing existing and improve banking, financial and other services and products of Bank B Bhd, its related companies or selected parties.”
Bank C

“Bank C Group may also use your personal information to market Bank C Group’s products, and services to you based on your interest and...”

“Our use of your information may also extend to other purposes... which may at our sole discretion be made available to our third party vendors, advertisers, affiliates or relevant third parties”
Bank D

“... the Bank does not warrant the security of any information transmitted by the Customer using the Bank’s Internet Banking Services. Accordingly, the Customer hereby accepts the risk that any information transmitted or received using the Bank’s Internet Banking Services may be accessed by unauthorised third parties and the Customer agrees not to hold the Bank liable for any such unauthorised access or any loss or damage suffered as a result thereof.”
What’s Now?

- Education is Key
- Establish a Committee/Task Force
- Establish a data protection compliance plan
- Designate at least a senior manager responsible for compliance
Cont...

- Data protection compliance as performance evaluation
- Undertake data protection self assessments
- Ask the right questions about data protection practices
- More importantly create a culture for data protection
Concluding Remarks

- Data Protection is not rocket science
- It is all about respect and common sense
- It is about striking a balance between the need of an organisation to process data and the privacy of the individual
- Good data protection is good business, good for all.
Some of my works..

- **Cyber Law: Policies and Challenges**
  - Butterworths Asia
  - (1999)

- **Privacy and Data Protection**
  - Sweet & Maxwell
  - (2002)

- **Internet Banking: Law and Practice**
  - LexisNexis UK
  - (2004)

- **Information & Communication Technology Law Legal & Regulatory Challenges**
  - Thomson Reuters
  - (2009)
A Professional Guide to Personal Data Protection Act 2010

Will be published by Thomson Reuters August 2010
THANK YOU

abmunir@um.edu.my
http://profabm.blogspot.com