UTeM

اونيۏرسيتي تيکنيکل مليسيا ملاک

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Always A Pioneer, Always Ahead

UTeM

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

MyUTeM

BITS 2523
Cyberlaw & Security Policy
Lecture 9

By

Mohd Fairuz Iskandar Othman, Phd

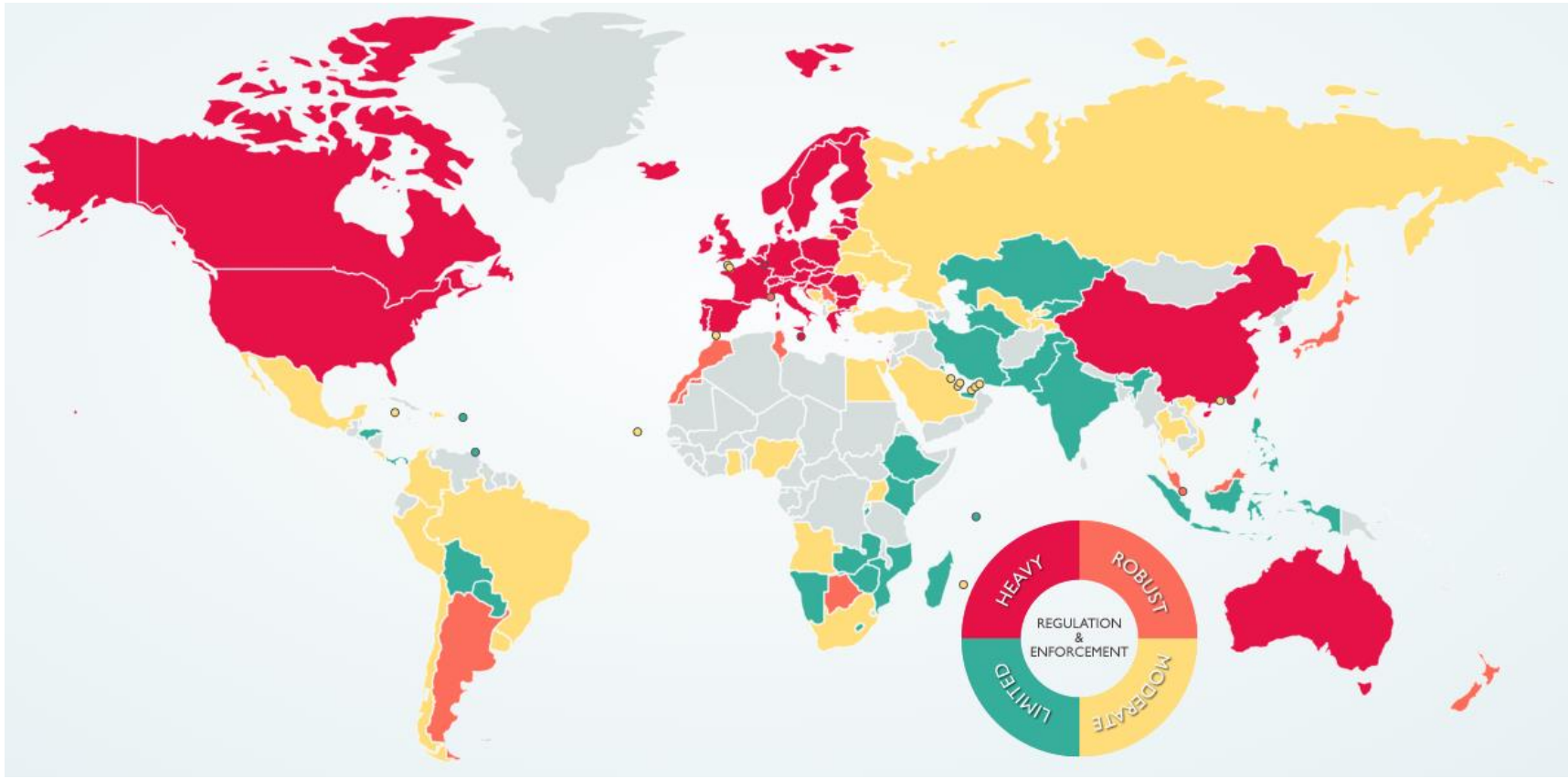
mohdfairuz@utem.edu.my

Personal Data Protection Act 2010

Topics covered:

- Definition
- Why do we need PDPA?
- Personal Data Protection Principles
- PDPA Enforcement
- Weaknesses & limitations
- Comparative influences
- Critique
- Summary
- Review Of Personal Data Protection Act 2010 (Act 709)

Data Protection Laws of the World



https://www.dlapiperdataprotection.com/index.html

PDPA Definition

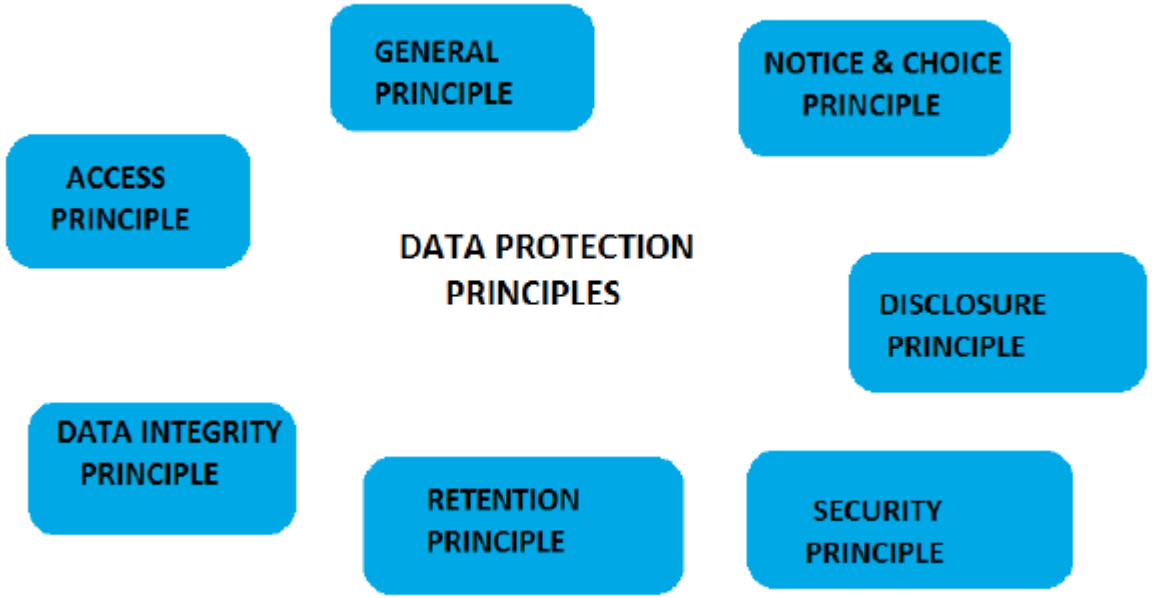
- PDPA is defined to mean any information recorded in a document in which it can practically be processed wholly or partly by any automatic means or otherwise which relates directly or indirectly to a living individual who is identified or identifiable from that information or from that and other information in the possession of the data user including any expression of opinion about the individual and any indication of the intentions of the data user in respect of that individual (Section 2 of the Malaysian PDPA Bill 1998).
- This definition includes any information or opinion of a living person that is identified or identifiable as personal data.
- The flaw of this definition is that it does not include other data, which may be used to identify a living individual.

Why do we need PDPA?

- The use of new technology is on the increase, and that potential breach may occur when personal information is acquired without consent or knowledge of the data subject.
- The fear of their data being misused us compounded by the fear that unscrupulous parties can gain access to their data by hacking the Internet companies they have transacted with.
- The anxiety about their personal data or confidential information getting into the wrong hands or even the hands of the Government is a major obstacle to more people going online.
- Malaysian consumers surveyed responded that security and privacy of their data was more important than convenience.
- Therefore, there is a need for laws and regulations pertaining to the security and privacy of personal data and information.

Personal Data Protection Principles

It is a requirement that a data user complies with all the data principles in processing personal data set out in Part II of the Act. These 7 principles are:



Principle 1: General principle

- A data user shall not process personal data about an individual unless that individual has given consent to the processing of their personal data.
- The personal data shall not, without the consent of the data subject, be disclosed except where the disclosure is for the purpose in connection with which it was collected or is directly related to data user's activity.

Principle 2: Notice and choice principle

- Where a data user is required to give a written notice informing an individual ("data subject") that their personal data is being processed by or on behalf of the data user, the notice shall, amongst other things, include the purpose for which the personal data is being collected and whether it is obligatory or voluntary for the data subject to provide the personal data.
- The notice must be given at the earliest opportunity when the data subject is asked to supply personal data.

Principle 3: Disclosure principle

- Any disclosure made under the Act must be in compliance with section 8.
- Personal data shall not, without the consent of the data subject, be disclosed for any purpose other than the purpose which was initially disclosed at the time of collection or to any party other than third parties for whom the data subject has given permission.

Principle 4: Security principle

- Security measures must be adopted in order to comply with Part II of the Act.
- Data users must take practical steps to ensure the security, reliability and integrity of the personal data.
- It is the duty of the data user to take all necessary steps to protect any loss, misuse, modification, unauthorised and accidental access or disclosure, alteration or destruction of personal data.

Principle 5: Retention principle

- Section 10 provides that the personal data processed cannot be kept longer than is necessary and the data user shall take all reasonable steps to destroy personal data that is no longer required.
- However, this provision does not specifically mention the life span of personal data.

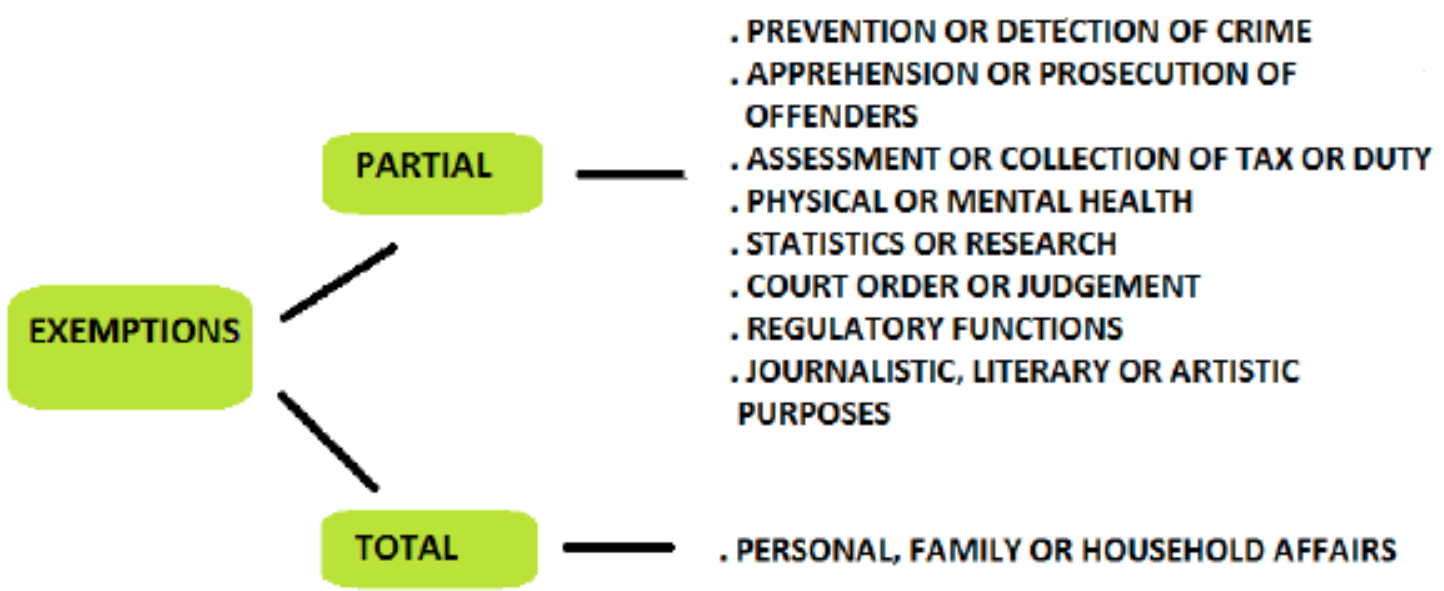
Principle 6: Data integrity principle

- Section 11 states that a data user must ensure that personal data is accurate, complete, not misleading and kept up to date, and related to the purpose for which it was collected.
- It is the duty of data user to guarantee the accuracy, completeness and correctness of the data collected.

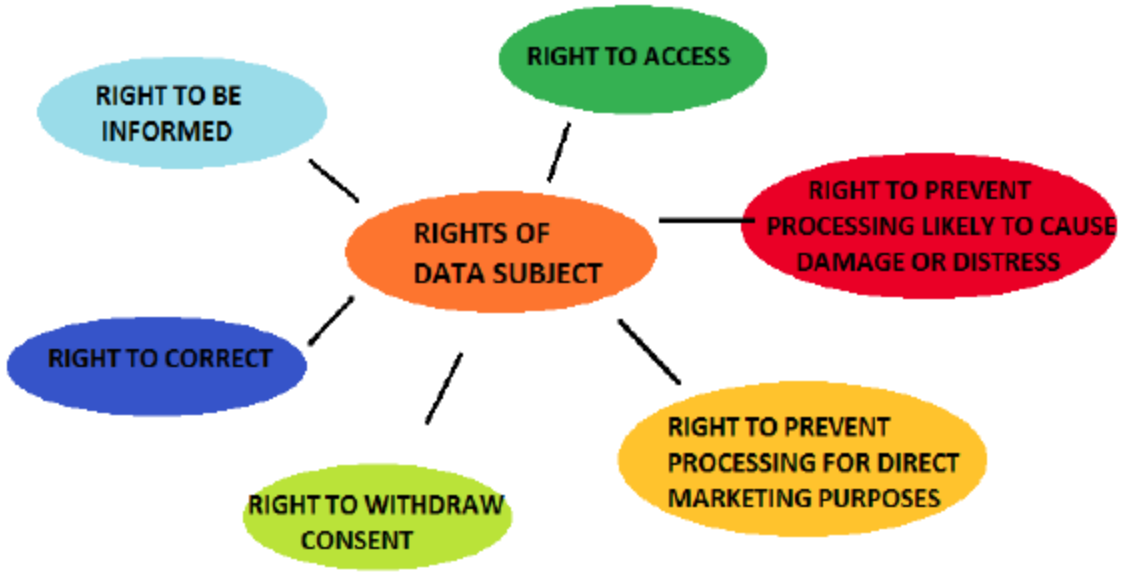
Principle 7: Access principle

- A data subject shall be given access to, and be able to correct, amend or delete personal data whenever it is inaccurate.
- However, access or correction can be refused under the Act.
- Thus, in any processing and handling of personal data it is mandatory for the data user to observe all data protection principles and any contravention of the principles results in an offence committed by the data user.
- Failure to abide by the above principles amounts to an offence. Upon conviction, the data user is liable to a fine not exceeding RM300,000 or to imprisonment for a term not exceeding two years or to both.

Exemptions to the 7 principles



Rights of data subject



PDPA Enforcement

- The Act provides for a Personal Data Protection Commissioner who is appointed by the Minister and who has various functions and powers particularly in implementing and enforcing the law.
- The Commissioner is responsible for advising the Minister on the national policy for personal data protection and carrying out all relevant actions in exercising the administration of personal data as set out in the Act and directed by the Minister. However, despite the wide functions and powers granted to the Commissioner under the Act, the Commissioner is responsible and answerable to the Minister.
- The Commissioner has an administrative duty to decide whether there is a serious breach of personal data protection principles through complaints made by any person regarding an act or practice that contravenes the Act. Upon receiving a complaint, an investigation will be carried out in accordance with section 105.

PDPA Enforcement (cont...)

- The Commissioner may refuse an investigation if he or she is of the opinion that there has been no contravention of the provisions of the Act. On completion of the investigation, when the Commissioner is satisfied that contravention of the provisions of the Act occurred, an enforcement notice as provided under section 108 will be issued.
- The Commissioner may later appoint an authorised officer to exercise the powers of enforcement under the Act. The decision specified in the enforcement notice can be challenged by filing a notice of appeal with the Appeal Tribunal. A decision of the Commissioner is not final. An aggrieved party may appeal to the Appeal Tribunal whose decision is final and binding on the parties to the appeal.

Criminal offenses

Weaknesses & limitations of PDPA 2010

1. Restriction to commercial transactions
2. Government not bound (the Act does not apply to the Federal and State governments.)
3. Commisioner's lack of independence
4. Personal data exclusions

Weaknesses & limitations of PDPA 2010 (cont...)

- By the definition, the data and confidential information of online consumers fall under the meaning of "commercial transactions" intended by the Act. Thus, if a customer provides their name, address, contact number and some other information to complete a transaction, that data or personal information is protected under the Act. The company receiving the information is under an obligation to keep the data and is allowed to use or disseminate the data only with the consent of the data subject.
- Conversely, the data of a patient in relation to medical treatment will not fall under this definition as it does not have commercial features. Nevertheless, that data merits similar protection for the reason that it is easily abused and misused through online transactions.
- Similarly, the PDP 2010 has no application to personal data collected through social media networking websites such as Facebook, Twitter and MySpace because that data is not as a result of commercial transactions. The fact that those data are being stored and kept by foreign online providers which do not have local centres of data processing justifies its exclusion from the scope of the Act.

Comparative influences

Among the influences for devising PDPA include:

- Hong Kong Personal Data (Privacy) Ordinance 1995
- UK Data Protection Act 1998
- Organisation for Economic Cooperation and Development (OECD) Guidelines 1980
- Council of Europe Convention for the Protection of Individual with regard to Automatic Processing of Personal Data 1981
- EU Data Protection Directive 1995
- APEC (Asia-Pacific Economic Cooperation) Privacy Framework 2004
- Madrid Resolution 2009

Critique

- The Personal Data Protection Act 2010 covers the private sector only – government agencies are exempt. The Personal Data Protection Act 2010 closely mirrors the principles in the European Union directive, with some variations that appear to adopt parts of the APEC Privacy Framework. However, the Act does not contain any European Union style registration requirements.
- The obvious shortcoming of the PDP Act 2010 is the definition of personal data.
  - Why it is confined to specified commercial transactions?
  - Why not make it more general to cover all purposes, as in other countries?
  - What protection is there for personal data of a non-commercial character?

Critique (cont...)

- These are the questions that become the central concerns in order to improve the Act so that it will cover all circumstances in which personal data is collected and processed. It is interesting to note that the Act applies only to commercial transactions while the precedents that inspired the Act are generally applicable to all purposes. Little information is protected while this definitional limitation remains.
- The non-applicability of the PDP Act 2010 to Federal and State governments, as highlighted by section 3, raises a question as to different standards governing data of public and private bodies.
- What kind of protection is available if the data user is dealing with the government in regard to the same data?
- The fact that the Act does not bind the government will result in double standards in the treatment of the same type of data. Interestingly, this is the only Act on data protection that excludes its applicability to the public sector.
- By having different standards, full protection over personal data is hard to achieve.

Critique (cont...)

- The ultimate end of protection – remedy for individuals – is absent from the Act. There is no provision in the Act for compensation for an individual whose data has been misused. Though correction of inaccurate information is granted under the Act, the main focus of the Act is on sanctions for breach.
- This might provide some deterrence against breach, but does not compensate the victim. Due consideration should be given to this matter to ensure fair treatment of data subjects because if the data user contravenes the Act, the fine or imprisonment that may be imposed may be little consolation to the data subject whose data has been processed or released without consent.
- The PDP 2010 should provide specifically for private remedies such as damages in terms of monetary compensation and injunctions to the data subjects affected as a result of a breach of privacy. This would encourage compliance and restrain further invasion. This is in line with the international precedents which provide compensation for individuals who have suffered distress caused by any contravention by the data controller

Critique (cont...)

- The position of the Commissioner, whose position is a body corporate placed under the Ministry. This shows a lack of independence in the execution of its function.
- Looking to the nature of the duties and powers assigned by the Act, the Commissioner should be independent and should be made accountable directly to the Parliament. As the Commissioner holds a very important position in relation to personal data protection issues, greater accountability is needed in discharging his duties.

Summary

- The Act indicates that the government is serious in dealing with an aspect of privacy protection, for instance personal data, despite its narrow and limited application. The preamble itself indicates the Act is confined to commercial transactions. This limited scope deviates from best international practice as well as from the two jurisdictions that Malaysia referred to when preparing the PDP 2010. It is believed that political expediency is one of the reasons why the PDP 2010 was passed as it is.
- The passing of the Act in a way becomes a platform to recognise the right to privacy or at least personal privacy, however it is not that simple as the Malaysian Constitution and the courts have not recognised privacy rights. It is clear from the reading of the Act that privacy protection is not the motive behind the introduction of the Act. In fact, the legislation is a set of rules which provides protection of commercial interests in data and enables Malaysia to participate internationally particularly in cases of trans-border flow of personal data.

Summary (cont...)

- It seems the Act was not intended to recognise the right to privacy, but rather the seriousness of the government in handling, processing and treating personal data is evidenced through the passing of the Act.
- The Act's effectiveness to fulfil the overall intention of data protection law might be achieved if the phrase "commercial transactions" is removed so the law can cover all purposes.
- The Act must also bind both public and private sectors to ensure fair treatment of personal data.
- Last but not least, a clear provision on compensation or injunction rights to the person who suffered damage must be included as part of remedies available.

Review Of Personal Data Protection Act 2010 (Act 709)

- Public Consultation Paper No. 01/2020: 14 February 2020 - 28 February 2020 (Public-Consultation-Paper-on-Review-of-Act-709_V4)
- Personal Data Protection Act 2010 (Act 709) which was enacted in 2010 serves the purpose to regulate personal data processing in the commercial transactions. After almost 10 years of operation, there are needs to further strengthen the enforcement and implementation of Act 709, taking into consideration the emerging issues on personal data protection impacting both data users and data subjects from the aspects of economic, social and technology. In recent years, there have been growing cases of data breaches involving the multi-type of data users from different sectors which leads to challenges in implementing and enforcing the personal data protection law.
- Therefore, the study to review Act 709 has been conducted in 2019 with the aim to focus on the effective implementation of Act 709 compared to other data protection laws internationally and to explore areas for improvements. The study saw the engagement of experts from the industries, regulators, government agencies and academicians in series of lab to bring forth and discuss the improvement ideas to strengthen the Act 709.

Review Of Personal Data Protection Act 2010 (Act 709)

- In the process of reviewing the act, Personal Data Protection Commissioner (PDP Commissioner) seeks to gauge the views and comments of the public through this public consultation paper. Feedbacks and comments should not be limited to the issues stated in the 'Points to be Considered' in each proposed item under Part I (1-22), as it only serve as guidance. Further to the views and comments, the suggestion can also state whether there is a need for a new provision, amendments to the as-is provisions, amendments to the regulations, or code of practice or issuance of guidelines.
- Individuals/parties that interested to participate in this public consultation may do so by:
  - i) Write your comment/feedback (concise and with justification) in Microsoft Word format, concerning a specific number of the paragraph and page number (if appropriate) of the proposal in Part I;
  - ii) Fill in your particulars in Part II;
  - iii) Email no. i) and ii) to pcpdp@pdp.gov.my no later than Friday, 28th February 2020.

Review Of Personal Data Protection Act 2010 (Act 709)

- This public consultation is open to anyone who has the interest to get involved in the process of the Act 709 review. **All submission should reach the Commissioner by 28th February 2020**. Please do not hesitate to contact afiza@pdp.gov.my or noreen@pdp.gov.my if you have any enquiry.

Thank you very much for your interest and participation.

Personal Data Protection Commissioner

Ministry of Communications and Multimedia Malaysia

Example cases

Example cases:

https://www.malaymail.com/news/what-you-think/2021/02/15/time-to-review-personal-data-protection-law-in-malaysia-hafiz-hassan/1950014

https://www.malaymail.com/news/malaysia/2020/11/19/your-personal-details-in-mysejahtera-app-safe-health-ministry-assures-malay/1924036

https://www.malaymail.com/news/malaysia/2020/11/20/personal-data-protection-dept-opens-investigation-papers-on-six-online-mone/1924636

https://www.malaymail.com/news/singapore/2020/11/20/probe-into-claims-singapore-based-muslim-pro-app-sold-user-data-to-us-milit/1924442

https://www.malaymail.com/news/malaysia/2020/10/14/data-protection-agency-clears-airasia-over-alleged-sale-of-customer-info-ab/1912564

Thank You

MyUTeM

www.utem.edu.my