

The pdp act 2010 in malaysia law company business partnership essay

[Law](#)



**ASSIGN
BUSTER**

General principle Personal data can only be processed if the data subject has given consent . The processing of the personal data must be for a lawful purpose and directly related to data user's activity . For example , consent of the employee must be given before any personal data about employee can be divulged by the employer . It is said that employee has given his consent if the employee has been informed about the disclosure of his personnel data and no objection for him. The limitation is regarding non-application of the Act in the public sector which stated application to the federal and state governments are being exempted from the provisions of the PDPA. This raise enormous implication since various departments of public sector such as the Inland Revenue department and the Immigration department are two of the largest collectors and processors of personal data in Malaysia. Due to this, the critique of the author is instead of safeguarding the interests of data subjects but the PDPA is being enacted to legitimize data processing practices of the government. Notice and choice principle Data subject must be informed in a written notice when personal data is being processed . The Act allows the notice to be given as soon as practicable at the time of collection of personal data. However , notice must be given for related class of third party that data user shall disclose . For example , if the employer is processing the personal data of the employee , he must give written notice to the data subject to inform him the choices offered to him to a limit of the processing of his personal data. The critique from the author in this principle is that the Act only applies commercial transactions either contractual or not in the processing of personal data. Description of personal information is a useful commodity either to be processed by an organization or by individual

in the commercial transaction. Disclosure principle Personal data shall not be disclosed unless the data subject consents for any purpose other than the purpose indicated at the time the data is collected or other directly related purposes . In addition , personal data shall not be disclosed except the data subject consents to any other person other than the class of third parties stated in the written notice . For example , the employer shall not disclose information of the employee without his consent beyond its original purpose , unless the employee gives his consent for his data to be disclosed not less than the original purpose. A critique was raised up in which the federal or state government involves a third party contractor to perform a particular service in the collection of personal data. The third party contractor is the private sectors are not exempted by the Act as they have an added obligation to be bound by the terms of contract services with the government and shall not disclose personal data. The private-party contractor are not allowed to hide governmental exemption of provision in the Act. Security principle The data user must take practical steps to protect personal data from loss , misuse , modification , unauthorized or accidental access . Whether practical steps have been taken depend on the nature and type of the personal data , the potential harm if it is not protected , the location where the personal data is stored , the security measures adopted and the measures taken to ensure that personnel who have access to personal data are reliable , competent and have integrity . For example , these requirements ensure the employee data are secure such as no loss , misused , modified , destroyed or accessed accidentally during data processing . Data can be subject to cyber-attacks or viruses in the era of ICT

where commonly management are conducted electronically . Therefore , highest standard of security is a need to protect employees' data. Lack of independence and powers of enforcement by the Commissioner can be seen in Section 59 of PDPA which states that the Commissioner shall be responsible to the Minister and in return the Commissioner receives directions of a general character consistent with the provision in the Act. Due to these , the integrity of data protection law has been undermined and also weaken the protection of the individuals' data privacy. Retention principle Personal data shall not be kept longer than necessary for the fulfillment of the purpose of collecting and processing. Data user must take reasonable steps to ensure personal data is destroyed or permanently deleted if no longer required for the purpose of which it was processed. For example , the duration for which the data is kept should not be longer than necessary. The employer has to expect to keep the employees' data for the same period as in the employment contract which lasts for a long period according to the legal requirement in the Employment Act 1955. However , the employer has no longer to permanently keep the employee's personal data after he has retired or ended his employment. Data integrity principle Data user must take reasonable steps to ensure the personal data is to be accurate , complete , not misleading and kept up-to-date by having directly related purpose that the data was collected and processed. For example , the accuracy of the data depends on the input receivable by the employer. However , distress or damage to the employee happens when the received data is incorrect. Employer has to immediately do correction on the data. Access principle Data subject must be provided access to his data so as

to allow correction on the personal data and can refuse request by complying with the Act's provisions on refusing request. For example , under the Act , employees are given the opportunity to be allowed to access to their personal files and correct his personal data. In the era of ICT , employees can access their personal files by way of secret passwords in which their data are kept in electronic files for the electronically savvy management. According to Bakar Munir and Siti Hajar (2010) , this principle applies in relevant filing system which defines as any set of information relating to individuals that give specific information relating to particular individual is easily and readily accessible and are allowed to make correction on the personal data.