

**Majlis Peguam  
Bar Council Malaysia**

[www.malaysianbar.org.my](http://www.malaysianbar.org.my)

15, Leboh Pasar Besar  
50050 Kuala Lumpur, Malaysia  
Tel : +603-2050 2050  
Fax : +603-2026 1313, 2034 2825, 2072 5818  
Email : [council@malaysianbar.org.my](mailto:council@malaysianbar.org.my)

BC/P/17/2014

**Tuan Haji Abu Hassan Bin Ismail**  
**Ketua Pengarah**  
Aras 6, Kompleks Kementerian Komunikasi dan Multimedia  
Lot 4G9, Persiaran Perdana, Presint 4,  
Pusat Pentadbiran Kerajaan Persekutuan  
62100 PUTRAJAYA

**16 APR 2014**

By Hand

Dear Sir,

**Comments to the Personal Data Protection Commissioner's Proposal Papers**

**Comments to the Personal Data Protection Commissioner's Proposal Papers:-**

- (1) Guideline on Compliance for Personal Data Protection Act 2010 (PDPA); and**
- (2) Guide on the Management of Employee Data Under PDPA**

We refer to the above matter and the above Proposal Papers.

As requested by the Commissioner, our comments to the Proposal Papers are as follow:-

**Proposal Paper on the Guide on The Management of Employee Data Under the PDPA**

1. The Proposal Paper has made it clear that the PDPA applies to employee data. It would be helpful if the Guide also further defines the scope of the term "*employee*". For example, other than current employees, does the term also cover former employees, job applicants (successful and unsuccessful), trainees/apprentices and employees on probation?
2. We note personal data processed as part of the performance of a contract is exempted from the consent requirement. However if sensitive personal data is collected as part of the performance of the employment contract, do we presume that consent would still have to be obtained explicitly?

In an employment context, sensitive personal data is often collected eg. health related data for medical benefits, or criminal data when assessing suitability for employment, and therefore it would mean that employers would still need to take the step of obtaining sign offs for such sensitive personal data, despite the "performance of a contract" exemption.

3. It would be helpful if further good practice recommendations are provided with respect to the personal data protection principles. In particular:-

- **General Principle:** What does the exception for the “performance of a contract” cover when in the context of an employment relationship?

For example, where HR systems are consolidated as part of a central system- does consent have to be obtained for this, or would it be possible to rely on the exception to the consent required in that the personal data collected is collected as “part of the performance of a contract”?

- **Notice & Choice principle:** We presume that all the elements in Section 7 of the PDPA would apply to an employee data Notice and not just the 3 items listed in the Guide.
- **Disclosure Principle:** Further, how detailed must the list of disclosures to third parties be? Would it be sufficient to name general groups ie. “service providers” or must each entity to whom data is disclosed to be named, bearing in mind that it may not be practical or possible to name every single entity to whom the personal data is disclosed to?

Kindly also clarify as to whether or not consent has to be obtained when the personal data collected from the employees are transferred to the employer’s parent company, subsidiaries, related or associated companies, business partners, affiliates, clients and third party service providers for personnel/employee administration, work, secondment and general business management purposes.

- **Security Principle:** Storage of personal files in a “locked cabinet” may not be feasible in this day and age when most records are kept electronically. Further, what kind of security measures would be considered as adequate? Must the electronic files be encrypted, with such folders limitation access to those who need-to-know only?
- **Retention Principle:** Does this mean that personal data should only be kept for as long as allowed under applicable laws? Ie. 6 years under employment laws?

Please also clarify the various forms in which the personal data of employees may be received/retained, ie writing, electronically or verbally? If personal data is collected verbally, how does an employer ensure compliance under this principle?

- **Data Integrity Principle:** It would be helpful to have further guides as to how employers can keep personal data up to date and accurate. If the employer has facilities such as intranet or employee accounts whereby the employee can update certain details on their end, would this suffice?

4. Under the PDPA, personal data processed for the purposes of investigations are exempted from the provisions of the Act. Does the term "investigations" include internal workplace investigations conducted by employers for employee misconducts or arising from breaches of laws and regulations by employees?

#### **Proposal Paper on the Guideline on Compliance of the PDPA**

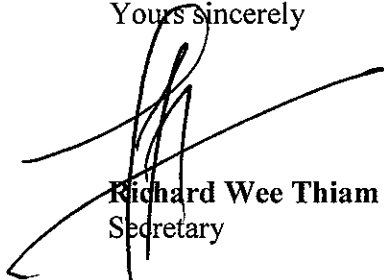
5. Business contact details such as name, office email address, company name, office address, office phone number and office fax number, shareholders & directors data (that can easily be obtained from CCM search)- are these information covered under PDPA? Or does the Act target only individual consumers? Note that the exception for consent (paragraph 6(2) of the PDPA Act) does not cover situations such as when the information is publicly available or when the information is necessary for performance of contract to which the employer of the data subject is a party.
6. Please also clarify if personal data of representative/liaison person of corporate customers/clients is also caught under the PDPA. What about personal data of deponents (individuals) who sign affidavits or statutory declaration on behalf of their employer companies who are the data users' corporate customers/clients?
7. In respect of the method of providing the notice under the Notice and Choice Principle,- please clarify on the acceptable methods. Must the data user strictly comply with s. 136 of the PDPA? Is sending a website url address (linking to the privacy notice) to the data subject by way of email/ sms sufficient? Or is notice uploaded on the website sufficient itself without the need to send website url address by email/sms to data subject?
8. As for designated compliance officer to be responsible for the data protection, would the failure to appoint such an officer amount to an offence, or is this merely a best-practice recommendation? Further, must a dedicated person be employed to be the compliance officer or is an officer who holds other roles being sufficient to take on the role of compliance officer?
9. It would be helpful if further Guidelines are issued on what is expected of data users, in terms of security and data integrity measures, as well as indication of retention periods which would be acceptable. We presume that data may be retained for as long as required to comply with existing laws ie. income tax laws, limitation periods etc.
10. In terms of the Notice & Choice principle, it would be helpful if certain practical guidelines are drawn up to explain how detailed the Notice should be, eg. would it be sufficient to name general groups ie. "service providers" or must each entity to whom data is disclosed to be named, bearing in mind that it may not be practical or possible to name every single entity to whom the personal data is disclosed to.

11. In respect of the list of third party disclosures that must be kept by data users, how detailed is this list required to be? Must each third party be named in this list?

We look forward to hearing from you.

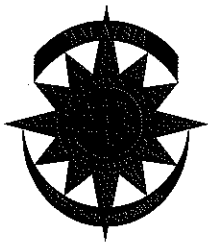
Thank you.

Yours sincerely



**Richard Wee Thiam Seng**  
Secretary

\\bar\_dc\practitioner's affairs\ad-hoc committee on pdpa\letters to be sent\response to proposal papers (clean).docx\germaine



**Majlis Peguam  
Bar Council Malaysia**

BC/P/17/2014

www.malaysianbar.org.my

15, Leboh Pasar Besar  
50050 Kuala Lumpur, Malaysia  
Tel : +603-2050 2050  
Fax : +603-2026 1313, 2034 2825, 2072 5818  
Email : council@malaysianbar.org.my

**Tuan Haji Abu Hassan Bin Ismail**  
Ketua Pengarah Jabatan Perlindungan Data Peribadi  
Jabatan Perlindungan Data Peribadi  
Aras 6, Kompleks Kementerian Komunikasi dan Multimedia  
Lot 4G9, Persiaran Perdana, Presint 4,  
Pusat Pentadbiran Kerajaan Persekutuan  
62100 PUTRAJAYA

**19 MAY 2014**

By Hand

Dear Sir,

**Feedback and Opinion on the Proposal of the Personal Data Protection Department to establish an Advisory Guideline Related to Consent Requirement under the PDPA (“Consent Guidelines”)**

---

1. The Consent Guidelines appear to introduce new exceptions to the consent requirements:
  - (a) To prevent injury or other damage to the health of the data subject; or
  - (b) For the performance of any other function of a public nature performed in the public interest by a person; or
  - (c) For the purpose of legitimate interests pursued by a data user except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject;

Further clarity is required on how these new exceptions gel with the PDPA and whether the Consent Guidelines will have the force of law. Further clarity is also required on the scope of the exceptions, particularly as the third exception uses the term “legitimate interests”, which could be given a very wide interpretation.

Consent

2. The Consent Guidelines also appear to contradict the PDP Regulations 2013, r.3(1) which stipulates that consent must be capable of being recorded. **The PDP Regulations suggest that express consent is required** whereas the Consent Guidelines state *“This would mean that consent may vary not only from case to case*

*but also between implied and explicit insofar as processing of sensitive personal data is concerned. Hence, the key test will be the ability to demonstrate that consent exists or being given by the data subject.”*

- The inconsistency should be resolved and it would also be helpful if further elaboration is given on factors to be considered when determining whether implied consent is acceptable
- The Commissioner should clarify whether consent can be given after the processing starts. 3<sup>rd</sup> parties may provide personal data of individuals to the data user without the data user’s prior request or without the data user soliciting for such personal data.
- The Commissioner should also clarify whether confirmation of consent is considered as “recordable consent” as provided in the PDP Regulations. An example of “confirmation of consent” is when the data subject provides a verbal consent and the data user writes to the data subject to confirm that he or she had provided his or her consent
- It would be helpful if the Commissioner can clarify whether verbal consent is acceptable and how it should be recorded. For example:-
  - whether confirmation in writing with the individual subsequent to the verbal confirmation is considered as "recordable form"; and
  - where appropriate (e.g. the data subject does not provide a correspondence address), whether a written note (which may be in electronic form or other form of documentary evidence) of the fact that an individual had provided verbal consent
- It would also be helpful if the Commissioner can clarify whether consent through a data subject’s non-verbal act or acts not capable of being recorded are acceptable and if not, how it should be recorded. For example, when the data subject drops his business card on a bowl for the data user’s promotional use.
- The Commissioner should set out exceptions to the “recordable consent” condition, in particular, where it is impracticable to obtain such recordable consent or confirmation of consent.

“ability to demonstrate”

- What does the “ability to demonstrate” mean? Does it mean that it has to be recorded in a form that can be kept? Or just recorded in a form that the Data User is aware that the Data Subject had consented to the usage of his/her personal data?

“recorded”

- It would be helpful if the Commissioner would state in what recorded form consent should be given. Whether it should be in written form, oral form or electronic form.
- If it is in written form, would emails and text messages qualify as written form?
- In respect of electronic portals, would the recording of personal data submitted through a click of a button qualify as the data subject’s consent?
- A proper definition of written form should be given

“consent exist”

- What kind of factual evidence is necessary to demonstrate that consent exists?
- The Consent Guidelines also contradicts the PDPA which clearly stipulates that explicit consent is required before processing of sensitive personal data. Further clarity on how this gels with the PDPA is therefore necessary.

3. The Consent Guidelines highlight that *“it is important for data users to ensure that a data subject is fully aware of and understands the purposes for which his/her data are being processed. It states Consent can be understood to have been given when individuals do not object or volunteer their personal data after the purposes of processing are clearly explained. Nevertheless, a clear explanation by trained staff of the data user is necessary to prove that consent has been obtained from the data subject after the purposes of processing have been explained.”*

“fully aware”

- The word “fully aware” goes beyond the meaning of mere consent
- This seems to suggest that the Data Subject would need to really understand and/or have full knowledge as to what his/her personal data is being used for.
- The standard for this would be much higher compared to merely getting the consent of the Data Subject.
- What standard should be imposed here?
- Doesn’t the point of “fully aware” negate implied consent? And if it does, would that mean that personal data which is processed as part of the performance of a

contract which is exempted from the consent requirement would now require express consent to be given?

- Exemptions or guidelines should also be given to circumstances where the data user has no direct contact with the data subject.

“When individuals do not object”

- Would this mean that when they do not object, consent is impliedly given? If so, it goes against what was said above that the data subject must be fully aware and understands the purpose for which the personal data is being used.
- What is the position now? Does there always have to be express consent for every circumstance or can consent be implied as well?

“Understands nature and effect of such consent”

- Does this statement mean that explicit consent is required?

“Purposes of processing”

- However, there is no elaboration on the factual evidence required to show that the purposes of processing have been clearly explained.

Need for Trained Staff

- Firms were informed earlier by the PDP department that Data Protection officers were not needed however this paper seems to contradict that position.
- What about smaller firms that do not have the necessary resources or time to train their limited staff to deal with the workload that would need to go into preparing themselves to brief and/or take questions dealing with PDP. How would these firms cope? Would the department give the relevant employees of the firm the proper training required?
- Also, what level of training is required for staff to be considered as “trained staff”?



- How is the staff supposed to explain the relevant PDP details to the data subject? Would it be through verbal communication and/or email and/or text messaging and/or over the phone?
- This new requirement is not reasonable and too onerous

#### **Consent on Behalf of 3<sup>rd</sup> parties**

4. The Consent Guidelines also appears to be inconsistent with the Personal Data Protection Regulations, which stipulate that consent must be obtained from a parent/guardian/person with parental responsibility for minors. However, Paragraph 5 of the Consent Guidelines suggests that consent for minors may be given by any relative (e.g. uncle, aunty, brother, sister) whether or not they have legal guardianship. Further clarity is required on this point and a wider group should be given in regards to consent by 3<sup>rd</sup> parties.
5. The Commissioner should clarify whether consent is required for personal data provided by a 3<sup>rd</sup> party. For example, a list of the said party's employees.
6. The Commissioner should also clarify whether a warranty provided by a 3<sup>rd</sup> party that consent had been obtained is sufficient to show "recordable consent". There may be a scenario where it is impracticable to obtain written consent from each and every data subject.

#### **3<sup>rd</sup> parties' personal data processed for the purpose of or during the provision of legal services**

7. The Commissioner should **expressly** state that the 3<sup>rd</sup> party's personal data processed for the purpose of or during the provision of certain legal services by an advocate and solicitor do not require consent. For example, statements to state that consent is not required for:-
  - scenarios where an advocate and solicitor prepares for litigation or a transaction e.g. credit checks, conflict checks, surveillance by the advocate and solicitor or private investigator;
  - litigation purposes (whether or not an action has been filed in Court), particularly when collecting information about an opposing party for the purpose of advancing a party's case; or collected during a discovery application.
  - personal data tendered or that may be tendered in Court for the purpose of legal proceedings.

### **Failure to Opt Out**

8. The Commissioner should clarify whether failure to opt out would constitute consent or would depend on the facts and circumstances of each individual case and what are the factors to be considered.

### **Publicly available data**

9. The Commissioner should clarify whether publicly available personal data such as personal data of directors and shareholders obtained from the Companies Commission of Malaysia or even social media websites such as Facebook can be used without the individual's consent or used for limited circumstances, which include legal proceedings.

### **Personal Data processed inadvertently**

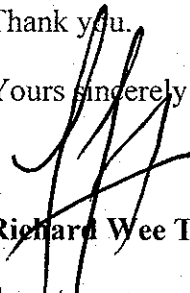
10. The Commissioner should address whether the processing of personal data processed inadvertently require consent. For example, in scenarios where:-
- A lawyer obtains document containing personal data of parties other than his client;
  - A photographer captures a photograph of a public space for commercial use with the faces of other individuals visible

### **Personal data processed prior to the enforcement of the PDPA**

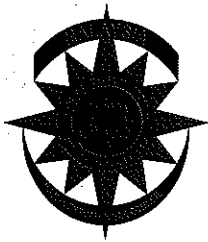
11. The Commissioner should clarify whether recordable consent is required for personal data processed prior to the enforcement of the PDPA. We take the view that it is impracticable and too onerous to have such recordable consent.
12. If so, whether a data user should obtain consent when the services to the data subject had already been completed and there are no further dealings with the data subject.

Thank you.

Yours sincerely

  
**Richard Wee Thiam Seng**

Secretary



**Majlis Peguam  
Bar Council Malaysia**

BC/P/17/2014

**Tuan Haji Abu Hassan Bin Ismail**  
Ketua Pengarah Jabatan Perlindungan Data Peribadi  
Jabatan Perlindungan Data Peribadi  
Aras 6, Kompleks Kementerian Komunikasi dan Multimedia  
Lot 4G9, Persiaran Perdana, Presint 4  
Pusat Pentadbiran Kerajaan Persekutuan  
62100 PUTRAJAYA

www.malaysianbar.org.my

15, Leboh Pasar Besar  
50050 Kuala Lumpur, Malaysia  
Tel : +603-2050 2050  
Fax : +603-2026 1313, 2034 2825, 2072 5818  
Email : council@malaysianbar.org.my

01 AUG 2014

By Hand

Dear Sir,

**Feedback and Opinion on the Proposal of the Personal Data Protection Department to establish a Guide on the Management of CCTV under the PDPA (“CCTV Guidelines”)**

1. The CCTV Guidelines state that *“an individual’s image is also identified as personal data and will be subjected to PDPA when it is involved in a commercial transaction such as for promotion or sale of products and services either by contract or otherwise.”*

*“commercial transaction”*

- Further clarity is required as it is unclear as to what kind of CCTV recording is subject to the PDPA. Does this mean that all CCTV recordings made on business premises or premises where a commercial transaction is likely to be carried out will be subject to the PDPA? Or can it be argued instead that CCTV recordings are made solely for security purposes, for the detection and prevention of crime and not made for a commercial transaction (i.e. images or footage are not going to be sold) and therefore will not be subject to the PDPA?

**Consent**

2. The CCTV Guidelines also state that for purposes other than personal data processed for the prevention or detection of crime or for the purpose of investigation, *“consent is required from an individual for any of his/her images recorded are to be used in commercial transactions”*. This will appear to contradict the PDP Regulations, *“which stipulate that consent must be capable of being recorded”*, as the PDP Regulations suggest that express consent is required but it would not be practicable to obtain *“recordable consent”* from each and every individual whose image is captured via the CCTV recording, which will also require the data user to provide a Privacy

Notice, which is mandated to be in writing, to fulfill eight (8) requirements, and in two (2) languages, to the individual.

- The inconsistency should be resolved and it would also be helpful if further elaboration is given on what kind of consent will be required and guidance on how such consent can be obtained.
- It would be helpful if the Commissioner can clarify whether consent through a data subject's non-verbal act or acts not capable of being recorded are acceptable and if not, how it should be recorded. For example, when the data subject notices the CCTV camera on the premises of the data user but does not question or object to it.
- The Commissioner should also clarify the position where a data subject is not involved in a commercial transaction with the data user but happens to appear in the frame of the CCTV recording, for example, as a passer-by.

3. The CCTV Guidelines highlight that under the Notice and Choice Principle, *"it is the responsibility of organizations or the owner of premises installed with CCTV to display a notice that is visible to the visitors and placed at the entrance to the CCTV surveillance zone, informing them of the CCTV operation and the purposes for installation"*.

*"display a notice"*

- What else should be explained in the notice apart from informing the visitors of the CCTV operation and the purposes for installation? Should this notice also contain other information required to be contained in the written notice, eg. contact details of the person responsible for personal data of the organization?
- In what language should this notice be displayed? Will it be sufficient to only be in the English language or will it also be required to be in the Malay language?
- What standard should be imposed to the notice being displayed? Is it merely a condition that it is "visible" or should the notice be "brought to the attention" of the visitors?

*"visitors"*

- The word "visitors" seems to contradict the application of the CCTV Guidelines, which state that an individual's image will be subjected to the PDPA when it is involved in a commercial transaction, as it is unlikely that all visitors to the premises will be involved in a commercial transaction. Again, this goes back to

the need for clarification of the application of the CCTV Guidelines and clarification of its definition of a “commercial transaction”.

4. The CCTV Guidelines also mention that *“individuals have the right to view their own images captured upon their request. However, procedures for access along with necessary details from the individual should be provided explicitly by the organization to confirm his/her request for access to his/her images only.”*

“access”

- How will access be dealt with? Is there an industry standard that should be adhered to? This will be highly onerous, if not impossible, to locate the image of the data subject in a crowd upon hours of footage.
- Further, in reviewing and providing such access to the individual, there is the risk of exposing footage of other people and their images/identity to the person seeking access. How will this be managed?

We trust our comments above may initiate constructive discussion in this matter and look forward to meet Tuan. Haji Abu Hassan Bin Ismail and your team for any other discussions/ dialogues on matters relating to PDPA.

Thank you.

Yours sincerely



**Richard Wee Thiam Seng**  
Secretary

\\bar\_dc\practitioner's affairs\ad-hoc committee on pdpa\letters to be sent\24.7.2014\feedback and opinion [24 July 14].docx