TENAGA NASIONAL BERHAD
(199001009294 (200866-W))

SABAH ELECTRICITY SDN. BHD. (462872-W)

sarawak energy

PERSONAL DATA PROTECTION CODE OF PRACTICE FOR THE UTILITIES SECTOR (ELECTRICITY) VERSION 2.0

21ST JANUARY 2020

PERSONAL DATA PROTECTION CODE OF PRACTICE FOR THE UTILITIES SECTOR (ELECTRICITY) VERSION 2.0

21ST JANUARY 2020

PESURUHJAYA PERLINDUNGAN DATA PERIBADI

Ref. No.
CoP_UTL(E)V2

IN exercise of the powers conferred by Section 23(3) of the Personal Data Protection Act 2010 (Act 709), I hereby register the Code of Practice for the Utilities (Electricity) Class of Data Users and it is applicable to all data users under the said Class with immediate effect.

Dated: 21 January 2020

(ROSMAHYUDDIN BIN BAHARUDDIN)
Personal Data Protection Deputy Commissioner, Malaysia

PESURUHJAYA PERLINDUNGAN DATA PERIBADI

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Background

1.1.1 The Personal Data Protection Act 2010 ("PDPA"), which came into effect on 15 November 2013, requires a separate code of practice for each specific class of data users.

1.1.2 In this Personal Data Protection Code of Practice for the Utilities Sector (Electricity) Version 2.0 ("CoP"), certain words are used. The meaning of those words are explained in Part 2 (Definitions) of the CoP.

1.1.3 The Personal Data Protection Commissioner ("PDP Commissioner") recognises that each Data User has different business practices and operates from different business locations. The PDP Commissioner grants each Data User the discretion and general flexibility to respond to issues arising under the CoP, provided that the PDP Commissioner must be consulted before any Data User implements any action outside the scope of the CoP. The PDP Commissioner shall notify the Data User of any decision within reasonable period after consultation, failing which, it is deemed approved by the PDP Commissioner.

1.1.4 The CoP is developed by the Data User under Section 23(1)(b) of the PDPA and is applicable to the Utilities Sector (Electricity) namely Tenaga Nasional Berhad ("TNB"), Sabah Electricity Sdn. Bhd. ("SESB") and Syarikat SESCO Berhad ("SESCO") with the approval of the PDP Commissioner and taking into consideration the views of the Energy Commission of Malaysia and the Ministry of Utilities Sarawak.

1.1.5 Subject to compliance of the CoP, TNB, SESB and SESCO shall regard the CoP as defence against any action, prosecution or proceeding whether by way of litigation, administrative tribunal or alternative dispute resolution for one or more alleged breaches under the PDPA. Such defence shall also be applied to a place outside Malaysia that do not have data protection, specific legislation or if the legislation is not considered as adequate in relation to Processing of Personal Data.

1.2 Objective of the CoP

1.2.1 The CoP is aimed to:

(a) set and outline standards of conduct for the Data User in respect of the Processing of Personal Data;
(b) ensure reasonable steps are taken in order to ensure that the Processing of Personal Data does not infringe Data Subject's rights; and
(c) establish a guideline to oversee and enforce compliance of the Data User.

1.2.2 The Employees and Data Processors such as contractors, suppliers, vendors, consultants and other service providers should be aware of:

(a) the seven (7) Principles of the PDPA;
(b) the way Personal Data should be processed;
(c) security requirements whilst Processing Personal Data; and
(d) non-compliance of the PDPA in the event if they fail to comply with the CoP.

1.3 Scope of the CoP

1.3.1 The CoP shall apply to the following:

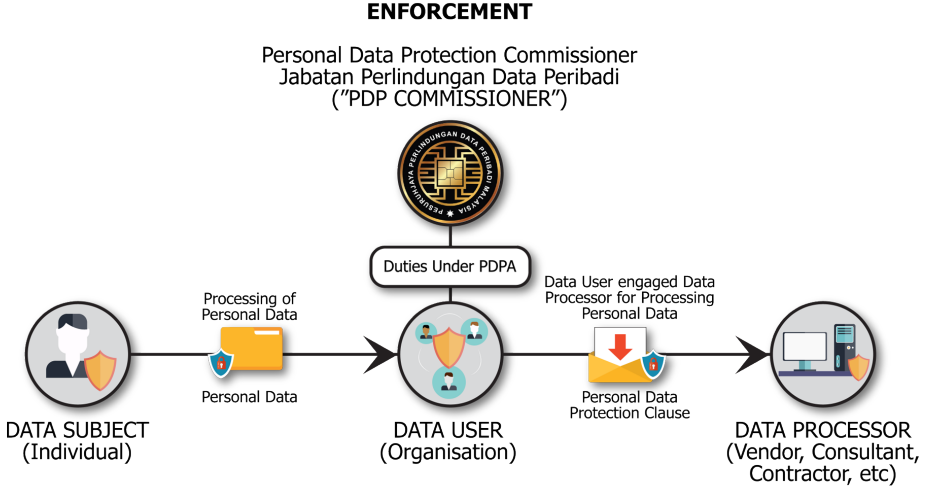
(a) Data User and Data Subject;
   i. consumer of the Data User;
   ii. Relevant Person;
   iii. individual who has been identified as a potential consumer of the Data User;
   iv. individual who has applied to be a consumer of the Data User; and
   v. individual who has entered into an ancillary arrangement with the Data User (e.g. guarantors or third party undertaking) on behalf of the Data Subject or entity;

(b) Data User and Data Processor;

(c) Data User and Employees, including an individual who has submitted any job application(s) with the Data User; and

(d) individual who visits the Data User's premises.

1.3.2 A diagrammatic illustration of the relationships between Data Subject, Data User, Data Processor and the PDP Commissioner are as follows:



1.3.3 Compliance with the PDPA will support the Data User's Commercial Transactions, and it is the duty of the Employees and the Data Processors such as contractors, suppliers, vendors, consultants and other service providers to comply with the CoP.

1.3.4 Different penalties apply for different offences under the PDPA as per Appendix I in which upon conviction carry a maximum fine not exceeding RM500,000 or to imprisonment for a term not exceeding three (3) years or both.

1.3.5 The Data User is under the obligation to comply with the CoP. The non-compliant Data User may be subjected to a fine not exceeding RM100,000 or to imprisonment for a term not exceeding one (1) year or both as stipulated under Section 29 of the PDPA.

1.3.6 In the event of any conflict between the CoP with:

(a) any laws, rules or regulations applicable to the electricity supply industry; or
(b) the terms or conditions of any licence or approvals issued or conditions imposed by the industry regulator,

the Data User is expected to comply with all laws, rules and regulations applicable to the electricity supply industry and all terms and conditions of any license or approvals granted or imposed by the industry regulator.

1.3.7 In the event of any conflict between English and national language (Bahasa Melayu) versions of the CoP, the English version shall prevail.

1.3.8 Examples provided in the CoP are not intended to be exhaustive but are included for context and purposes of illustration.

1.4 Certificate of Registration (Regulation 8 of the Personal Data Protection (Registration of Data User) Regulations 2013)

1.4.1 The Data User shall display a certificate of registration and any amendment to the certificate, if any, at a conspicuous place at the principal place of business and a certified copy by the PDP Commissioner of the certificate of registration for each branch, where applicable.

1.4.2 A "branch" means any office operated by the Data User where interaction occurs with the Data Subject. However, kiosks, offices where there is no interaction with the Data User, premises operated by marketing agents or dealers and premises of the Data Processor are not considered to be a branch for purposes of the CoP.

1.4.3 Failure to display the certificate of registration constitutes an offence liable to a fine not exceeding RM10,000 or to imprisonment for a term not exceeding one (1) year or both.

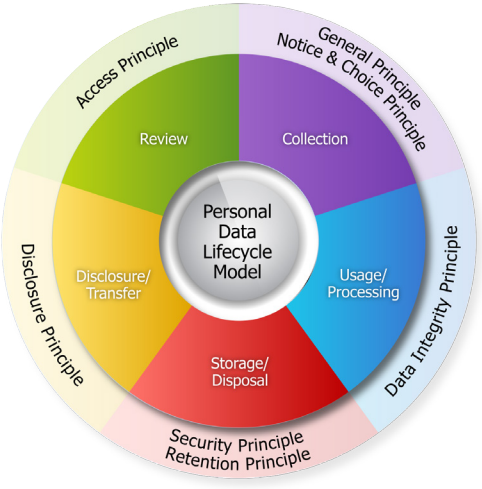
1.5 Personal Data Life Cycle Model

1.5.1 The CoP has been structured taking into consideration the seven (7) PDPA principles, namely General Principle, Notice & Choice Principle, Disclosure Principle, Security Principle, Retention Principle, Data Integrity Principle and Access Principle, under the five categories of the Personal Data Lifecycle Model as stated below:

No.	PERSONAL DATA LIFE CYCLE/ ACTIVITIES	7 PDPA PRINCIPLES
1.	Collection	General Principle
		Notice & Choice Principle
2.	Usage/ Processing	Data Integrity Principle
3.	Storage/ Disposal	Security Principle
		Retention Principle
4.	Disclosure/ Transfer	Disclosure Principle
5.	Review	Access Principle

1.5.2 The Personal Data lifecycle relates to the day-to-day data Processing activities. These are linked to the seven (7) PDPA principles based on the purpose of Personal Data Processing. The seven (7) PDPA Principles are to be cross-referred collectively, instead of, in isolation depending on the purpose of Personal Data Processing activities.

1.5.3 A diagrammatic illustration: Personal Data Lifecycle Model.



2. DEFINITIONS

For the purpose of the CoP, the various words and terms used throughout the CoP shall have the same meaning as per the PDPA, unless specified otherwise.

Words	Meaning
Collect	In relation to Personal Data, an act by which such Personal Data enters into or comes under the control of the Data User.
Commercial Transactions	Any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a credit reporting business carried out by a credit reporting agency under the Credit Reporting Agencies Act 2010.
Data Access Request ("DAR")	Written request made by a Requestor to the Data User to access Personal Data of that Data Subject, using the Data Access Request Form, as set out in Appendix II.
Data Correction Request ("DCR")	Written request made by a Requestor to the Data User to correct Personal Data of that Data Subject, using the Data Correction Request Form, as set out in Appendix III.
Data Processor	In relation to Personal Data, any person, other than an Employee of the Data User, who processes Personal Data solely on behalf of the Data User, and does not process Personal Data for any of the Data Processor's own purposes.
Data Subject	An individual who is the subject of the Personal Data.
Data Subject Notice	A Written notice by the Data Subject to request the Data User to cease or not to begin the Processing if it causes or is likely to cause substantial damage or distress to him or another person.
Data User	A person who either alone or jointly or in common with other persons processes any Personal Data or has control over or authorises the Processing of any Personal Data, but does not include a Data Processor. Data User under the CoP are: (a) TNB; (b) SESB; and (c) SESCO.

Direct Marketing	Communication by whatever means of any advertising or marketing material which is directed to particular individuals.
Disclose	An act by which such Personal Data is made available by the Data User.
Employee/ Employees	Employees of the Data User which include: (a) a person appointed to serve the Data User under a contract of service and/or contract for service; (b) a person who is transferred or seconded to or by the Data User for the purpose of employment; and (c) industrial trainees or trainees.
Federal Government	The Government of Malaysia, which includes all the ministries and the Prime Minister's Department.
Minister	Minister in charge with the responsibility for the protection of Personal Data pursuant to the PDPA.
Official Identification Documents	(a) Identity Cards such as MyKad, MyPR, MyKAS or MyTentera; (b) Passport; or (c) other valid documentary proof of identity.
PDP Notice	A written notice (howsoever described) by the Data User to a Data Subject, in both the national and English languages, that the Data User is required to make available to the Data Subject in compliance with Section 7 of the PDPA.
PDP Regulations	(a) Personal Data Protection Regulations 2013; (b) Personal Data Protection (Class of Data Users) Order 2013; (c) Personal Data Protection (Registration of Data User) Regulations 2013; (d) Personal Data Protection (Fees) Regulations 2013; (e) Personal Data Protection (Compounding of Offences) Regulations 2016; (f) Personal Data Protection (Class of Data Users) (Amendment) Order 2016; and

	(g) Personal Data Protection Standard 2015, including any amendment to the PDP Regulations and any new subsidiary legislation(s) published in the Gazette.
Personal Data	Any information in respect of Commercial Transactions, which: (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a Data Subject, who is identified or identifiable from that information or from that and other information in the possession of the Data User, including any Sensitive Personal Data and expression of opinion about the Data Subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.
Processing	In relation to Personal Data, means collecting, recording, holding or storing Personal Data or carrying out any operation or set of operations on Personal Data, including: (a) the organisation, adaptation or alteration of Personal Data; (b) the retrieval, consultation or use of Personal Data; (c) the disclosure of Personal Data by transmission, transfer, dissemination or otherwise making available; or (d) the alignment, combination, correction, erasure or destruction of Personal Data.
Relevant Person	In relation to a Data Subject, howsoever described, means: (a) in the case of a Data Subject who is below the age of 18 years, the parent, guardian or person who has parental responsibility for the Data Subject;

	(b) in the case of a Data Subject who is incapable of managing his own affairs, a person who is appointed by a court to manage those affairs, or a person authorised in writing by the Data Subject to act on behalf of the Data Subject; or (c) in any other case, a person authorised in writing by the Data Subject to make a DAR, DCR, or both such requests, on behalf of the Data Subject.
Requestor	A Data Subject or Relevant Person for the purpose of DAR and DCR.
Sensitive Personal Data	Any Personal Data consisting of information as to the physical or mental health or condition of a Data Subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister may determine by order published in the Gazette.
State Government	Government of a state which includes the state secretary's office and state department(s).
Third Party or Third Parties	Any person other than: (a) a Data Subject; (b) a Relevant Person in relation to a Data Subject; (c) a Data User; (d) a Data Processor; or (e) a person authorised in Writing by the Data User to process Personal Data under the direct control of the Data User (e.g. contractor, consultant, supplier or vendor).
Vital Interests	Matters relating to life, death or security of a Data Subject.
Writing or Written	All electronic or non-electronic method of recording information, which includes type writing, printing, lithography, photography, electronic storage or transmission (e.g. via electronic channels) or any other method of recording information or fixing information in a form capable of being preserved (e.g. digital voice recordings).

3. COLLECTION

3.1 Types of Data

3.1.1 The types of data that may be processed by the Data User include but are not limited to:

Personal Data	Sensitive Personal Data	Non Personal Data
• Name • Address • Gender • Date of birth • Telephone number • Fax number • Citizenship • Bank account • Email address • Web browsing information (cookies, IP address, the time, date and duration of visit) • Official Identification Documents • Photograph or video image • Audio recording • All other information, whether verbal or Written, which identifies the Data Subject • Employee personal information • All other contact details or information related to any of the abovementioned items.	• Physical or mental health or condition of the Data Subject such as medical record • Political opinion • Religious beliefs or other beliefs of a similar nature • Commission or alleged commission of any offence(s) and/or disciplinary • Racial or ethnic origin • Biometric information • Fingerprint.	• Amount of electricity bill • Electricity consumption • Data relating to a company, society, partnership, organisation or any other legal entity • Electricity bill payment history • Electricity tariff • Data relating to deceased persons • Aggregated and/or anonymised data (no name basis) wherein the person is non-identifiable.

3.2 Sensitive Personal Data (Section 40 of the PDPA)

3.2.1 Processing of Sensitive Personal Data is only allowed under any of the following circumstances:

(a) the Data Subject has given explicit consent;
the following examples are deemed that explicit consent has been given by the Data Subject:

***Example (a1)**: By signing or marking at the relevant part of the application form, signifies the Data Subject's explicit consent for the Data User to process his Sensitive Personal Data.*
***Example (a2)**: The conduct of the Data Subject by voluntarily providing his Sensitive Personal Data to the Data User such as submitting a copy of his identity card for employment or obtaining services from the Data User.*
***Example (a3)**: Any verbal consent by the Data Subject to process Sensitive Personal Data which is recorded by the Data User (for example via audio recording) signifies that explicit consent has been given by the Data Subject.*

(b) if the Processing is necessary for any of the following purposes:

i. for the performance or exercising of any right or obligation which is conferred or imposed by law on the Data User in connection with employment;

ii. in order to protect the Vital Interests of the Data Subject or another person, in a case where consent cannot be given by or on behalf of the Data Subject or the Data User cannot reasonably be expected to obtain the consent of the Data Subject;

iii. in order to protect the vital interests of another person, in a case where consent by or on behalf of the Data Subject has been unreasonably withheld;

iv. for medical purposes and is undertaken by a healthcare professional or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare professional;

v. any legal proceedings;

vi. obtaining legal advice;

vii. establishing, exercising or defending legal rights;

viii. administration of justice;

ix. exercise of any functions conferred on any person by or under any written law; or

x. for any other purposes as the Minister thinks fit; or

(c) the information contained in the Personal Data has been made public as a result of steps deliberately taken by the Data Subject.

3.2.3 Non-compliance with the PDPA in Processing the Sensitive Personal Data, may result in a fine not exceeding RM200,000 or to imprisonment for a term not exceeding two (2) years or both, as stipulated in Section 40(3) of the PDPA.

3.3 Collecting and Processing Personal Data (Section 6 of the PDPA)

3.3.1 Personal Data must only be collected or processed:

i. for a lawful purpose directly related to an activity of the Data User;

ii. necessary for or directly related to that purpose; and

iii. adequate but not excessive in relation to that purpose.

***Example (a)**: Collection of Personal Data by IT department in order to set-up new users on the Data User's IT systems.*
***Example (b)**: Job applicant should provide reference details such as name, contact number and designation to the Data User.*

3.3.2 The purpose of collecting Personal Data should be clear. Procedures should be adopted to ensure that only relevant information is processed i.e. the information held is necessary to meet the Data User's business objectives.

***Example**: Name, contact number, premises address and Identity Card number are the information relevant for electricity supply.*

3.3.3 The Data User must be able to justify the collection and Processing of Personal Data, whereby the Data User should only Collect information that is relevant and not excessive in relation to the purpose for which it is collected.

***Example (a)**: The Data User should not Collect bank account details from job applicants except when they have commenced their employment with the Data User.*
***Example (b)**: When submitting an application form for electricity supply, the Data Subject must provide bank account details for the purpose of refund of security deposit, and this will not be considered as excessive.*
***Example (c)**: For the purpose of security, visitor should provide Official Identification Documents and telephone number in order to enter the Data User's premises and this will not be considered as excessive.*
***Example (d)**: Should there be any need by the Data User for its Employees to undergo activities for employment purposes, this will not be considered as excessive. Examples include providing fingerprint, undergo medical check-up including urine test and body mass index.*

***Example (e)**: For the purpose of training during the course of employment, disclosure of the Employee's Official Identification Documents number and/or telephone number to the relevant training provider is not excessive.*

3.3.4 Collecting or retaining Personal Data on the grounds that it may possibly become useful in the future is not acceptable.

***Example (a)**: Human Resource Department should only process Personal Data for human resource purpose only and based on the applicable retention requirements policy. For any new purpose of Processing, Human Resource Department should clearly state the purpose to ensure that the Data Subject provides sufficient information to fulfil such new purpose.*

***Example (b):** Retention of unsuccessful applicant's resume without consent from such applicant for future use is considered unnecessary retention of Personal Data and therefore it is not allowed.*

3.3.5 The Data User should never Collect, or hold or ask for information just because it may come in handy as this would be considered excessive and irrelevant.

3.4 Consent

3.4.1 The Data User cannot Collect or process a Data Subject's Personal Data without the Data Subject's consent.

3.4.2 Form of consent: Explicit or implied consent.
Consent either explicit or implied, must be acquired in a method that can be recorded and maintained by the Data User. For example:

i. signature or clickable box indicating consent;

***Example**: By clicking the "Agree" button through online application, it indicates that the Data Subject has provided consent for the Processing of Personal Data.*

ii. consent by conduct/ performance: consent is considered as given by way of conduct/ performance if:
   (a) the Data Subject does not object to the Processing;
   (b) the Data Subject voluntarily discloses his Personal Data; or
   (c) the Data Subject proceeds to use the services of the Data User;

***Example**: Consent is given by the Data Subject upon providing a copy of Official Identification Document, whether or not it contains Sensitive Personal Data to the Data User.*

iii. verbal consent: should be recorded either digitally (such as, through the use of call logger and/or recorder software) or by issuing a Written communication (such as issuing a letter, a form or an email from the Data User's official email) to the Data Subject confirming that consent has been given.

> ***Example**: Consent is given by a caller to the Data User to process the caller's Personal Data when the caller calls the Data User's customer service for their services.*

3.4.3 Any consent given on behalf of a Data Subject to the Data User shall bind the Data Subject if given by:

(a) the parent(s), legal guardian(s) or person(s) who has parental responsibility for the Data Subject, if the Data Subject is under the age of 18; or

(b) a person who is appointed by a court to manage the affairs of the Data Subject or a person authorised in writing by the Data Subject to act on behalf of the Data Subject.

3.4.4 For transactions between the Data User and a company, society, partnership, organisation or any other legal entity (collectively referred to as "the Legal Entities") which involves any Personal Data, it is the Legal Entities' responsibilities to obtain prior consent from a Data Subject. For avoidance of doubt, the Legal Entities shall warrant that consent from the Data Subject has been obtained in accordance with the PDPA.

> ***Example**: When submitting the Vendor/ Contractor Registration Application Form or Tender Document(s), the applicant or tenderer may Disclose Personal Data of their shareholder(s), proprietor(s), director(s), manager(s), administrator(s) or employee(s). Such disclosure to the Data User shall be deemed consented by the Data Subject(s).*

3.4.5 Exception to Consent

Consent is not required if the Processing is necessary for the following purposes:

(a) for taking the steps at the request of the Data Subject with a view to enter into a contract;

> ***Example (a1)**: The Data Subject must enter into an electricity supply contract for the purpose of applying electricity supply to the Data Subject's premises. For entering such contract, the Data Subject must provide necessary Personal Data such as name, identity number and premises address to the Data User. In this situation, the Data User is not required to obtain consent from the Data Subject.*

> ***Example (a2)**: Prior to entering into the electricity supply contract, the Data Subject must provide copy of supporting document containing Personal Data such as land title, sale and purchase agreement or tenancy agreement. As such, the Data User is not required to obtain consent from the Data Subject.*

***Example (a3)**: Consent is not required when the Data Subject appointed a contractor on behalf of the Data Subject in the submission of electricity supply application.*

(b) for the performance of a contract to which the Data Subject is a party;

***Example (b1)**: After entering the electricity supply contract, the Data User must perform obligations under the contract relating to the supply of electricity such as issuance of electricity bill and deliver it monthly to the Data Subject. As such, the Processing of Personal Data for issuance and delivery of the bill to the Data Subject, will not require consent from the Data Subject.*

***Example (b2):** For the performance of employment contract such as providing medical benefit, a Data Subject must submit medical report, upon request, to be processed by the Data User.*

(c) for compliance with any legal obligation to which the Data User is the subject, other than an obligation imposed by a contract;

***Example (c)**: The Data User to comply with request by the industry regulator such as to provide a copy of electricity supply contract for the purpose of investigating electrical accident at consumer's premises.*

(d) in the administration of justice;

***Example (d):** The consent from the Data Subject is not required, if the Processing is for the purpose of litigation, mediation, arbitration, conciliation proceedings or any similar in nature.*

(e) for the exercise of any functions conferred on any person by under any law; or

***Example (e1)**: The consent from the Data Subject is not required, if the Processing is to comply with the court order.*

***Example (e2):** The consent of the Data Subject is not required if the Processing is due to a written request made to the Data User, by the Federal Government or State Government or other law enforcement authorities, to provide Personal Data of the Data Subject, and such request is made pursuant to power or authority conferred under relevant law.*

(f) to protect the Vital Interests of the Data Subject (matters relating to life, death or security).

***Example (f)**: The consent of the Data Subject is not required if the Processing is due to the request by the Royal Malaysian Police or the Data Subject's immediate family in matters relating to life, death or security of the Data Subject.*

3.5 PDP Notice (Section 7 of the PDPA)

3.5.1 The Data User must Disclose their PDP Notice in the national and English languages to a Data Subject before or as soon as practicable after collecting and Processing of Personal Data. The PDP Notice will also be displayed on the website and in other locations where appropriate, such as offices or on mobile applications.

3.5.2 The PDPA does not require proof that the PDP Notice is received and/or accepted by a Data Subject.

3.5.3 The Data User may communicate the PDP Notice to a Data Subject by one or more of the following methods:

(a) posting a printed copy of the PDP Notice to the last known address of the Data Subject based on Data User's record;

(b) posting the PDP Notice on the website of the Data User;

(c) issuing a short message service (SMS) to the Data Subject with a website address/ link to the PDP Notice and/or a telephone number in order to request for the PDP Notice and/or further information;

(d) issuing an e-mail to the Data Subject with a website address/ link to the Data User's PDP Notice and/or telephone number to contact for further information;

(e) issuing an electronic message to the Data Subject providing a website address/ link to the Data User's PDP Notice and/or telephone number to contact for further information via such other electronic channels utilised by the Data User;

(f) inserting a summary notice in regular communications with the Data Subject (e.g. in monthly billing statements) with a website address/ link to the PDP Notice and/or a telephone number to contact in order to request for the PDP Notice and/or further information;

(g) prominently displaying a summarised version of the PDP Notice at the premises of the Data User's place of business (e.g. at the counter desk that the Data Subjects come to and/or at a prominent location in the Data User's premises), and making available the full PDP Notice either upon a request being made at the counter or to an Employee of the Data User;

(h) displaying a message on the screens of kiosks with a website address/ link to the PDP Notice, a telephone number to contact for further information and/or stating that the PDP Notice is available at the branch of the Data User;

(i) inserting a statement in application/ registration forms referencing the PDP Notice, which may be accessed at a given website address/ link, or by making a request to an Employee of the Data User, or by calling a telephone number provided in the application/ registration form;

(j) printing out copies of the PDP Notice and providing it to Data Subjects at the Data User's premises; or

(k) any other mode of communication that serves to bring PDP Notice to the Data Subject.

3.5.4 PDP Notice must contain the following information:

(a) a description of the Personal Data of the Data Subject that is being processed by or on behalf of the Data User;

(b) the purposes for which the Personal Data is being, or is to be collected and further processed;

(c) any information available to the Data User as to the source of that Personal Data;

Example (c): *The Data User may need to Collect copy of identity card to confirm the identity of a job applicant as part of the recruitment process.*

(d) the Data Subject's rights to request access and to request correction of the Personal Data and how to contact the Data User with any inquiries or complaints in respect of the Personal Data;

(e) the class of Third Parties to whom the Data User may Disclose the Personal Data;

(f) the choices and means that the Data User offers the Data Subject for limiting the Processing of Data Subject's Personal Data, including Personal Data relating to other persons who may be identified from that Personal Data;

(g) whether it is obligatory or voluntary for the Data Subject to supply the Personal Data; and

Example (g1): *It is obligatory for the Employee to provide their Personal Data to the Data User to facilitate the payroll process.*
Example (g2): *Taking part in an optional survey by the Employee is an example of voluntary Processing.*

(h) where it is obligatory for the Data Subject to supply the Personal Data, the consequences for the Data Subject if Data Subject fails to supply the Personal Data.

4. USAGE / PROCESSING

4.1 Data Integrity (Section 11 of the PDPA)

4.1.1 When Processing Personal Data, the Data User shall take reasonable steps depending on the circumstances of each case to ensure the Personal Data held is accurate, complete, not misleading and kept up-to-date:

i. accurate – meaning that the Personal Data is captured correctly.

ii. complete – meaning that there is no omission of details in the Data Subject's Personal Data.

iii. not misleading – meaning that Personal Data processed should not be ambiguous, deceiving or an oversight.

iv. kept up-to-date – meaning that the Data User should ensure that the Personal Data is the latest data given by the Data Subject.

Example (a): *For electricity supply application, the Data User shall ensure that the Personal Data of the Data Subject such as name and identification card number are accurate as per the Data Subject's Official Identification Documents.*
Example (b): *The Data User may remind the Data Subject to update the Personal Data by notifying the Data Subject through any appropriate means of communication such as through the electricity bill or tax invoice and/or the Data User's corporate websites. But it is the responsibility of the Data Subject to notify the Data User of any changes to the Personal Data with relevant supporting documents.*
Example (c): *The Data User must ensure that the Personal Data of the visitors are recorded accurately as per Official Identification Documents and/or driving license.*
Example (d): *The Data User to notify its Employees to update their Personal Data from time to time.*
Example (e): *In the event that the complainant is reluctant to give his full name or details to the Customer Service after being requested by the Data User, the Data User is deemed to have complied with the Data Integrity Principle.*
Example (f): *The marital status of the Data Subject should not be falsely reflected by the Data User.*

Example (g): *The information recorded by the Data User must correctly reflect the information given by the Data Subject.*
Example (h): *The change of address made by the Data Subject must be recorded by the Data User.*

4.1.2 The following steps may be considered by the Data User to comply with the Data Integrity Principle:

(a) the Data User may require the Data Subject to inform the Data User of any changes to the Data Subject's Personal Data. The Data User will not be in breach of the Data Integrity Principle if the Data User is not informed by the Data Subject of changes to the Data Subject's Personal Data;

(b) the Data User will provide a DAR and/or DCR to access and update or correct the Data Subject's Personal Data at any branches of the Data User or at other points of contact with the Data Subject; and

(c) updating the Personal Data if the Personal Data is provided by the Data Subject/Relevant Person with relevant supporting documents to verify the identity of the Requestor.

4.1.3 The Data User will not be in breach of the Data Integrity Principle if the Personal Data provided by the Data Subject/Relevant Person is inaccurate, incomplete, misleading and not up-to-date.

4.1.4 The Data User need not update or correct the Data Subject's Personal Data based on information given by any party other than the Data Subject/Relevant Person.

4.1.5 The Data Integrity Principle will not be breached if:

(a) the Data User does not verify the validity of the supporting documents of the Personal Data given by the Data Subject/Relevant Person;

(b) the Data User retains all records in order to accurately reflect the reality in such cases as for historical record-keeping (e.g. previous addresses) and records of errors (e.g. the accurate recording of the event of the accidental termination of the Data Subject's account).

5. STORAGE / DISPOSAL

5.1 Security Principle (Section 9 of the PDPA)

5.1.1 The Data User shall when Processing Personal Data, take practical steps to protect the Personal Data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

5.1.2 The Data User shall take into consideration the following measures:

(a) Administrative;
   i. Confidentiality/Non-Disclosure Agreement;
   ii. periodic supervision/monitoring of Employees, as deemed appropriate by the Data User; and
   iii. suitable training/awareness plan for the Data User's Employees;

(b) Physical;
   i. door access system to control entry into and exit from premises where Personal Data is stored;
   ii. CCTV (if necessary);
   iii. 24 hours security monitoring (if necessary);
   iv. for Personal Data that is processed manually, the measures include:
      a. filing the Personal Data in an organised manner;
      b. keeping files containing Personal Data in locked storage facilities;
      c. keeping storage keys in a secure place/ area;
      d. recording the movement of storage keys; and
      e. documents should not be left unattended such as near printers or fax machines;

(c) Technical;
   i. access authorisation systems;
   ii. back-up/ recovery systems;
   iii. anti-virus and anti-malware software; and
   iv. limiting access to technologies (example: systems, applications or, social medias) which have the potential in disseminating the Personal Data,

to safeguard the confidentiality, integrity and availability of the Personal Data, whether processed electronically or non-electronically.

5.1.3 The Data User should implement security measures and control based on:

(a) the nature of the Personal Data;

(b) the level of sensitivity of the Personal Data; and

(c) the harm that could result from its loss, misuse, modification, unauthorised or accidental access, disclosure, alteration or destruction.

5.1.4 The Data User will also need to ensure the following reasonable steps are taken:

(a) access by authorised Employee;

Example (a): *Access to the Data User's premises or equipment must be on an as-needed basis and must not be given to anyone who is not an Employee of the Data User, unless agreed by an Employee authorised by the Data User.*

(b) the sharing of Personal Data with Third Parties;

Example (b1)*: Third Parties to whom Personal Data has been disclosed should agree not to Disclose Personal Data to unauthorised Third Parties.*
Example (b2)*: The Data User's Employee with access to Personal Data should not Disclose Personal Data to any Third Parties without a Confidentiality Agreement/ Non-Disclosure Agreement/ Letter of Undertaking.*

(c) the place or location where Personal Data is stored shall not be exposed to physical and natural threats;

Example (c)*: To store Personal Data on a higher ground in a flood prone areas to prevent exposure to natural threats.*

(d) security measures incorporated into any equipment in which Personal Data is stored;

Example (d1)*: Anti-virus, anti-malware and access authorisation systems should be deployed where appropriate.*
Example (d2): *Update the back-up/recovery system to prevent Personal Data intrusion and such.*

(e) the measures taken for ensuring the authority, reliability, integrity and competence of Employee having access to Personal Data;

Example (e1)*: A training or awareness programme for Employee shall be implemented.*
Example (e2)*: Upon termination of any contract, agreement or engagement, the Data User shall revoke and/or terminate any access by any parties (such as Employee or Data Processor) to Personal Data in timely manner to the following:*

i. The Data User's premises;
ii. Equipment;
iii. Network;
iv. Systems or applications; and
v. Electronic databases and non-electronic Personal Data storage.

(f) the measures taken for ensuring the secure transfer of Personal Data; or

(g) implementing disaster recovery plans and business continuity plans to protect and recover Personal Data against any possible disaster and business interruption.

***Example (g)**: Data Recovery Plan and Business Continuity Plan testing/simulation shall be conducted periodically to ensure mitigatable data recovery activity(ies) in the event of disaster.*

5.1.5 In the event of a Personal Data breach (e.g. unauthorised disclosure of Personal Data), the Data User:

(a) shall establish the potential harm caused by the breach incident to a Data Subject, and take proactive steps to contain the damage. The Data User should be able to demonstrate commitment and accountability when addressing the breach; and

(b) may notify the PDP Commissioner voluntarily if the breach is severe and risks reputational damage unless otherwise required by the legislation for the Data User to notify the PDP Commissioner.

5.2 Installation of CCTV

5.2.1 CCTV recordings may be made for the purposes of safety, security monitoring or investigation.

5.2.2 For any CCTV installed within the Data User's premises, a visible notice must be displayed in or outside the premises, informing the public of the CCTV operation and the purpose of its installation.

5.2.3 The CCTV notice shall:

(a) be in the national or English language;

(b) be visible and noticeable at the Data User's premises, especially within the CCTV surveillance zone; and

(c) describe the purpose of recording and contact details of the person responsible for CCTV recording.

5.2.4 A sample of the CCTV notice may appear as follows:

In English language:
Security Notice: These premises are under 24-hour CCTV camera surveillance. Images are recorded for the purpose of crime prevention and public safety. For further information, please contact [•].

In national language:
Notis Keselamatan: Premis ini adalah di bawah pengawasan 24 jam kamera CCTV. Imej dirakam adalah bagi tujuan pencegahan jenayah dan keselamatan awam. Untuk maklumat lanjut, sila hubungi [•].

5.3 Retention of Official Identification Documents

5.3.1 Before entering the Data User's premises, the Data Subject may be required to surrender the Data Subject's Official Identification Documents, driving licence or any other relevant document containing Personal Data acceptable and adequate to the Data User and it may be photocopied or scanned and retained by the Data User.

5.3.2 If Data Subject's Official Identification Documents is to be retained for a duration of which the Data Subject is in the Data User's premises, this must be done in accordance with the National Registration Regulations 1990, the Protected Areas and Protected Places Act 1959 and the Police Act 1967 and only an auxiliary policeman may do so.

5.4 Requirements for Engagement of Data Processor

5.4.1 If a Data Processor is appointed by the Data User, such as an outsourced service provider, vendor or supplier, it is recommended that the Data User uses reasonable efforts to include in its agreement with the Data Processor (whether in the form of a contract, letter or any formal written document):

(a) provision on confidentiality, non-disclosure and technical and/or organisational security measures;

(b) conditions under which Personal Data may be processed;

(c) representations, undertakings, warranties and/or indemnities which are to be provided by the Data Processor;

(d) security measures governing the Processing to be carried out as may reasonably be contained in the Data User's internal security policy and/or standards; and

(e) deletion, destruction and/or return of Personal Data that is under the control of the Data Processor upon completion or termination of the contract or engagement, unless the Data User decides otherwise.

***Example**: Security measures or controls should be implemented for high-risk Processing activities, may include but not limited to Robot Process Automation (RPA), Artificial Intelligence, Data Analytics and prospective emerging technologies.*

5.5 Retention and Disposal (Section 10 of the PDPA)

5.5.1 The Data User may only keep the Personal Data for as long as it is necessary for the purpose it was collected.

5.5.2 The Data User will take all reasonable steps to ensure that the Personal Data, whether electronically or non-electronically processed, is permanently destroyed or deleted when it is no longer required by the Data User.

***Example (a)**: To securely dispose of non-electronic documents which contained Personal Data once no longer required, by using shredder machine.*
***Example (b)**: To wipe clean Personal Data from electronic media once no longer required.*

5.5.3 In cases where the Data User needs to retain Personal Data beyond a specified statutory period, the Data User should be able to show a reasonable need to retain Personal Data beyond the applicable statutory period.

***Example**: The commencement of legal proceedings or investigations concerning the Data Subject would qualify as grounds for continuing to retain the Personal Data beyond the expiry of the retention period and may be retained until the final disposal/ closure of the matter.*

5.5.4 Personal Data may be retained as long as it is required for the following purposes:

(a) legal proceedings or a regulatory requirements or similar investigations or obligations to produce the said information;

(b) a crime is suspected or detected; or

(c) information is considered to be of potential historical importance,

provided that the Data User shall not use the Personal Data retained for any other purposes. This requirement applies to both manual and electronic copies of documents containing the Personal Data.

5.5.5 The Data User shall, take all reasonable steps to ensure that all Personal Data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed by having regard to the following:

(a) determine the retention period according to the relevant legislation relating to the Processing and retention of Personal Data are fulfilled before destroying the Personal Data;

(b) keep Personal Data no longer than necessary unless there are requirements by other legal provisions, including but not limited to Companies Act 2016, Income Tax Act 1967, Employment Act 1955, Sabah Labour Ordinance (Cap 67), Sarawak Labour Ordinance (Cap 76), Limitation Act 1953, Sarawak Limitation Ordinance (Cap 49), Sabah Limitation Ordinance (Cap 72), National Archive Act 2003, Enactment Record and Archive Sabah State 2007;

***Example (b)**: In accordance to National Archive Act 2003, the Employee's personal file should be retained by the Data User for 20 years as directed by the Director of National Archive after the personal file is no longer in use.*

(c) maintain a proper record of Personal Data disposal periodically and make such record available for submission when directed by the PDP Commissioner;

(d) dispose Personal Data collection forms used in Commercial Transactions within the period not exceeding fourteen (14) days, except if/unless the forms carry legal values in relation to the Commercial Transaction;

(e) review and dispose all unwanted Personal Data in the database;

(f) prepare a Personal Data disposal schedule for inactive data within a twenty-four (24) month period. The Personal Data disposal schedule should be maintained periodically; and

(g) the use of removable media device for storing Personal Data kept by the Data User is not permitted without Written approval from the top management of the Data User.

5.5.6 The Data User shall ensure that there is no premature destruction of documents which could result in inability to defend litigious claims, operational difficulties and failure to comply with any applicable laws and regulations.

5.5.7 The disposal of Personal Data will assist the Data User to maintain sufficient electronic and office storage space resulting in desirable working environment. Periodic reviews, and if appropriate, disposal of unwanted Personal Data in databases should therefore be performed by the Data User.

5.6 Disposal of Personal Data

5.6.1 Destruction is applicable to paper-based Personal Data and permanent deletion is applicable to electronic based Personal Data.

5.6.2 Personal Data which is physically archived is still subject to the provisions of the PDPA and will continue to remain so until it is destroyed, permanently deleted or anonymised. The Data User's retention policies should address restricted access to and destruction of Personal Data.

5.6.3 For Personal Data stored on an electronic medium, the permanent deletion of the Personal Data will require the electronic media (such as, hard drive or a removable media device) to be wiped clean once the Personal Data has been deleted. The Data User is to take reasonable effort to permanently delete the Personal Data from electronic media.

5.6.4 However, Personal Data may be retained for statistics or analysis basis provided that the Data Subject's Personal Data is not processed for any other purpose and that the resulting statistic is not made available in a form which identifies the Data Subject.

5.6.5 In the event of data disposal, a disposal record should be kept to evidence the act of the disposal.

6. DISCLOSURE / TRANSFER

6.1 Disclosure to Third Party (Section 8 of the PDPA)

6.1.1 The Disclosure Principle is related to the Notice and Choice Principle and for the purpose for which the Personal Data is collected.

6.1.2 The Data User shall not Disclose Personal Data of a Data Subject to Third Parties without the consent of the Data Subject, except as described in Clause 6.1.3 below.

> ***Example:*** *Bank request for Data Subject's Personal Data from Human Resource Department to proceed with confirmation of personal loan. Human Resource Department can only Disclose the requested Personal Data if the Data Subject had given consent.*

6.1.3 Exception to the Disclosure Principle

Even without the consent of a Data Subject, the Personal Data may be disclosed for the following purposes:

(a) the purpose for which the Personal Data was to be disclosed at the point of collection;

> ***Example (a)***: *In the process of supplying electricity, Data Subject's Personal Data has to be provided to the Third Party to whom the Data User has outsourced some of its data Processing activities.*

(b) for a purpose directly related to the purpose declared at the point of collection (for example, a purpose closely associated to the primary purpose); or

> ***Example (b1):*** *Data Subject defaults on his payment of electricity bill or tax invoice. The Data User discloses the relevant particulars of the Data Subject, including his debt amount to a solicitor or to a debt collection agent in order to recover the outstanding amount.*
>
> ***Example (b2):*** *Personal Data on the electricity bill or tax invoice may be disclosed to the outsourced meter reader, tenant, occupier of the premises, and to anyone who receives the electricity bill or tax invoice at the premises or at the address registered by the Data Subject.*
>
> ***Example (b3):*** *The electricity bill amount and/or consumption of the electricity (without the Data Subject's Personal Data) is not considered as Personal Data and may be disclosed to any Third Party for the purpose of payment.*

(c) disclosure to any permitted Third Parties as specified in Appendix IV. The Data User shall keep and maintain a list of disclosure to permitted Third Parties for the purposes of this paragraph in relation to Personal Data of the Data Subject that has been or is being processed by the Data User.

6.1.4 Disclosure to a permitted Third Party is subject to:

(a) an official letter from the permitted Third Party for the disclosure;

(b) name and relevant information of the respective Data Subject for identity verification;

(c) relevant provision of law in relation to the request of information; and

(d) purpose of the request under the following circumstances;

i. to prevent, detect and investigate a crime; (e.g.: specific section of the relevant Act);

***Example (d(i)1)**: Where there has been a security breach within the Data User's organisation or premises, the Data User may Disclose the information to a forensics specialist appointed by the Data User for internal investigation.*
***Example (d(i)2)**: Royal Malaysia Police requests from the Data User for CCTV recording for the purpose of preventing, detecting or investigation of a crime.*

ii. disclosure was required under the law or by a court order/ tribunal ordering the Data User to Disclose the Personal Data (e.g. court orders to Disclose Personal Data);

***Example (d(ii)1)**: If there is any court order to the Data User to Disclose Personal Data or any document that contains Personal Data, the Data User must comply with such order.*
***Example (d(ii)2)**: Disclosure of Personal Data as requested by Federal Government or State Government such as Royal Malaysia Police, Inland Revenue Department, Malaysia Anti-Corruption Commission for the purpose of preventing or detecting a crime, or for the purpose of investigation.*
***Example (d(ii)3):** Data Subject's Personal Data may be disclosed to the person listed in Rule 5(6) of the Licensee Supply Regulations 1990 for the purpose of refund of deposits by the Data User upon receiving a discharge and indemnity letter.*
***Example (d(ii)4)**: For the purpose of competency certification by Energy Commission ("EC"), copy of EPF Statement, passport photo, telephone number and other relevant information required by EC will be disclosed. Such disclosure is permitted as it is required by the industry regulator.*

iii. the Data User acted in the reasonable belief that the Data User had in law the right to Disclose the Personal Data to the Third Party;

***Example (d(iii)1)**: Where there is proclamation of sale, Data User may Disclose Data Subject's copy of electricity bills to the successful bidder and/or his solicitor.*

iv. the Data User acted in the reasonable belief that the Data Subject will consent; or

> ***Example (d(iv)1)****: If Data Subject is medically incapacitated, the Data User may Disclose the Data Subject's Personal Data to his immediate next of kin, guardian or authorized person subject to an indemnity agreement with the Data User.*

v. the disclosure was in the public interest as determined by the Minister.

6.2 Disclosure to Data Processor

6.2.1 The Data User must ensure that any disclosure to the Data Processor is governed by a contract/ agreement between the Data User and the Data Processor (e.g. contract meter reader or disconnection contractor, medical provider, system developer, service provider, security guard, vendor).

> ***Example****: A contract must be in place with an outsourced external security guard company who regularly records the Personal Data of visitors to the Data Users' premises.*

6.3 Internal Disclosure

6.3.1 Internal disclosure means disclosure or transfer of the Personal Data between business units within the Data User's organisation but excluding disclosure or transfer of the Personal Data to the Data User's subsidiaries and vice versa.

> ***Example:*** *For the purpose of salary payment, increment and bonus, the Human Resource Division may Disclose Personal Data to the Finance Division.*

6.3.2 Disclosure is permitted subject to:

(a) written application from the business unit; and

(b) disclosure of Personal Data is for official use only.

6.4 Disclosure or Transfer of Personal Data from the Data User to Its Subsidiary(ies), and Vice Versa

6.4.1 In certain circumstances and in order to perform its contractual obligation (if necessary and/or required), the Data User may Disclose or transfer the Personal Data to its subsidiary(ies) in

Malaysia and outside Malaysia for example, by having intra-group data transfer agreement on disclosure and/or transfer.

6.4.2 Such disclosure or transfer should be based on the original purpose of data Processing activity.

> ***Example:*** *The Data User's Human Resource Division Disclose and transfer Personal Data of Employees on secondment to its subsidiaries' Human Resource teams in the United Kingdom.*

6.4.3 The Data User may formulate global data sharing policy and standard operating procedures whilst operationalising such transfer.

6.5 Data User Acting as Data Processor

6.5.1 The Data User shall act as the Data Processor subject to present and/or future business model and process. In this circumstance, such subsidiary(ies) within the Data User may Disclose or transfer the Personal Data to the other Data User's subsidiaries for example, by having intra-group data transfer agreement on disclosure and/or transfer.

6.5.2 Such disclosure or transfer should be based on the original purpose or directly related to that purpose of Personal Data Processing activity.

> ***Example****: The Data User (acting as Data Processor) processes payrolls for its subsidiaries' employees, recruitment and transfers, contract management and payment to service providers.*

7. REVIEW AND RIGHTS OF DATA SUBJECT

7.1 Rights of Data Subject

7.1.1 The PDPA provides a Data Subject with the following rights as illustrated by the diagram below:

7.2 Right to Access Personal Data and Right to Correct Personal Data (Section 12 of the PDPA)

7.2.1 A Data Subject has the rights to request the Data User:

(a) to provide access to the Data Subject's Personal Data which is held by the Data User; and

(b) to correct the Data Subject's Personal Data held by the Data User which is inaccurate, incomplete, misleading, or not up-to-date.

7.2.2 Such requests can be made by the Requestor via the DAR form or DCR form respectively as per Appendix II and III. These forms are for reference purposes only and the Data User may revise or amend the forms according to their own business needs and where applicable.

> ***Example:*** *A spouse authorised by the Data Subject (being the Relevant Person) may request the Data User to access and/or update the Data Subject's Personal Data through the DAR or DCR form, whichever is relevant.*

7.2.3 The Data User is entitled to impose prescribed fees in accordance with the Personal Data Protection (Fees) Regulations 2013 for DAR. However, no fee will be imposed with respect to DCR.

7.2.4 The DAR or DCR form is not required under the following circumstances:

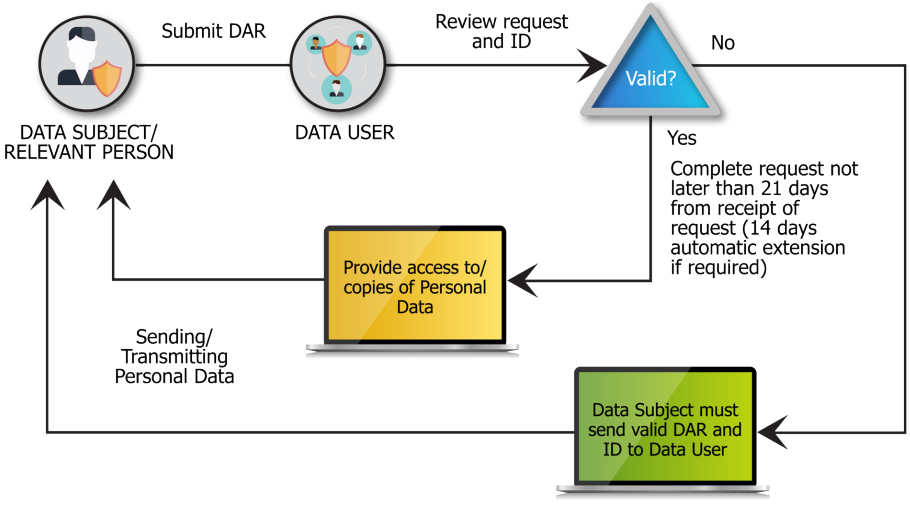
i. corporate consumer;

ii. the Data User's registered vendor/ contractor; and

iii. the Data Subject is able to access and/or update their Personal Data via the Data User's online platform.

7.3 DAR (Section 30 of the PDPA)

7.3.1 By way of diagrammatic illustration, the DAR process is as follows:



7.3.2 DAR Requirements (Section 31 of the PDPA)

(a) When submitting a DAR form as set out in Appendix II, the Requestor needs to satisfy the following:

i. submit a Written DAR form by way of email, fax, hand, post or any other official mode of communication used by the Data User;

ii. provide Official Identification Documents for verification purposes;

iii. pay the prescribed fee (if required);

iv. be specific as to the Personal Data that is being sought. (In this context, a request for "all Personal Data" is not considered a valid DAR);

v. provide relevant supporting documents as required;

vi. submit a separate DAR form for each account with the Data User that the Requestor is requesting access to; and

vii. if there is any request for a copy of the Personal Data by the Requestor, the Data User may charge the Requestor based on the prescribed fee.

(b) For purpose of clarity:

i if any one of the prerequisites above is not fulfilled, the Data User may return the DAR form to the Requestor and request for the omitted information, payment and/or copies to be resubmitted by the Requestor prior to acknowledging receipt;

ii in instances where the Data User receives a verbal request for access to Personal Data, the Data User is not required to respond to the request. However, the Data User should guide the Requestor on the proper manner of making a valid DAR and provide whatever assistance as may be required by the Requestor to make the DAR.

(c) When handling the DAR, the Data User will:

i. acknowledge receipt of the DAR form and provide to the Requestor, a copy of the Data Subject's Personal Data in an intelligible form within twenty-one (21) days of receipt of the DAR;

ii the Data User is to comply with the DAR within twenty-one (21) days from the date of receipt (i.e. date of acknowledged receipt) of the DAR. Where the initial twenty-one (21) days is insufficient, the Data User is required to inform the Requestor in Writing with the reason(s) for the delay before the expiration of the twenty-one (21) days. The Data User will be given an automatic extension of not more than fourteen (14) days to comply fully with the DAR; and

iii the Data User is to inform the Requestor in Writing once the copy of the Personal Data is ready for collection based on the Requestor's collection preference (i.e. at counter, post or email).

7.3.3 DAR Limitations

(a) The Requestor may only access the Data Subject's own Personal Data and must not be granted access to another person's Personal Data; and

(b) The Data User may utilise the following means of communication for audio and video recordings to the Requestor:

i. audio recordings may be communicated as written transcripts or provided in audio form; and/or

ii. video recordings (inclusive of CCTV images) may be communicated as a chronological set of image captures which are then printed, or as an edited video recording where all other Data Subjects' identities have been removed or masked.

7.3.4 Grounds for Refusal (Section 32 of the PDPA)

(a) The Data User has the right not to comply with or to reject the DAR if:

i. the Data Subject does not fulfill (if applicable) the requirements of completing the DAR form for each account which the request relates to, provide identification confirmation, pay the required fee, and/or provide sufficiently specific request;

ii. the Data User cannot comply with the DAR without disclosing Personal Data relating to another individual who can be identified from that information unless that other individual has consented to the disclosure of the information to the Requestor or it is reasonable in all the circumstances to comply with the DAR without the consent of the other individual;

iii. the Data User is not supplied with such information as reasonably required to locate the Personal Data;

***Example (a1)**: Requestor has requested access to Data Subject's CCTV images but has not identified the date, time, place and other relevant information of the visit and/or did not provide copy of relevant police report.*
***Example (a2)**: Requestor has requested access to audio recording of Data Subject's call to the Data User's call center but did not indicate the date and approximate time of Data Subject's call.*

iv. the burden or expense of providing access to the Personal Data is not proportionate to the risk to the Data Subject's privacy in relation to Personal Data (for example, if the time and cost to be incurred by Data User is greater than the significance of the Personal Data requested under DAR);

v. if the DAR is made to the Data User but the Processing of the Personal Data is controlled by any other data user to which the Data User is in such a way is prohibited from complying with the DAR, whether in whole or in part, except to any extent that the Data User can comply with the DAR without contravening the prohibition concerned;

vi. providing access would violate a court order or other legal prohibition;

vii. providing access would Disclose confidential commercial information;

viii. such access is regulated by any other law(s) other than the PDPA (such as laws or regulations relating to the supply of electricity);

ix. the relevant Personal Data is not available (such as if damaged due to unforeseen circumstances);

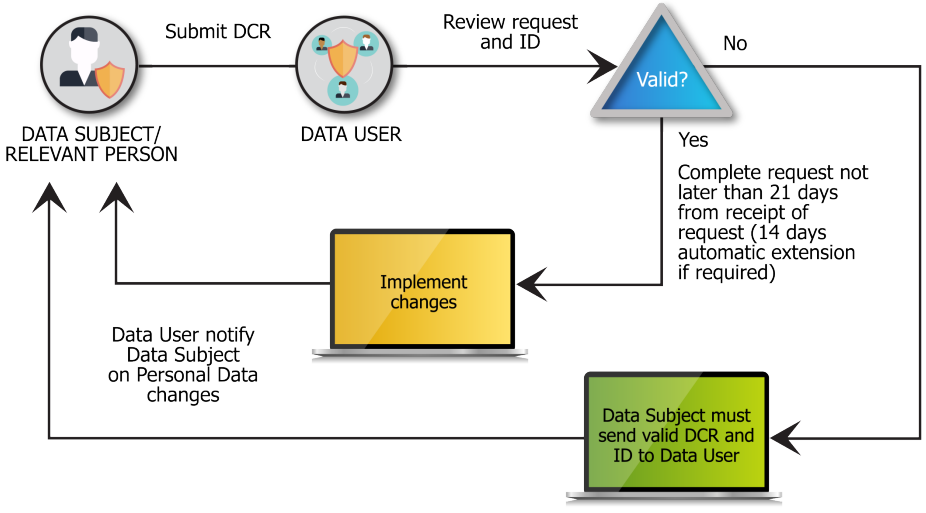
x. the request comes outside the retention period for the relevant Personal Data; or

xi. the request is a repetition of an earlier request.

(b) The Data User must provide to the Requestor a Written notice of the refusal to comply together with reasons in the event the Data User is unable to comply with the DAR within 21 days from the date of receipt of such DAR.

7.4 DCR (Section 34 of the PDPA)

7.4.1 By way of diagrammatic illustration, the DCR process is as follows:



7.4.2 DCR Requirements (Section 35 of the PDPA)

(a) The Requestor may submit a DCR form to the Data User to correct Data Subject's Personal Data at the Data User's premises, if:

i. after receiving a copy of the Personal Data from the Data User, the Requestor considers that Data Subject's Personal Data is inaccurate, incomplete, misleading or not up-to-date; or

ii. Data Subject knows that Data Subject's Personal Data (kept by the Data User) is inaccurate, incomplete, misleading or not up-to-date.

(b) When submitting the DCR form as set out in Appendix III, the Requestor needs to satisfy the following:

i. submit a Written DAR form by way of email, fax, hand, post or any other official mode of communication used by the Data User;

ii. provide Official Identification Documents as required for verification purpose; and

iii. provide supporting documents (if required) before any correction can be done by the Data User.

7.4.3 When handling the DCR, the Data User will:

(a) comply with the DCR within twenty-one (21) days from the date of receipt (i.e. date of acknowledged receipt) of the DCR form. Where the initial twenty-one (21) days is insufficient, the Data User is required to inform the Requestor in Writing with the reason(s) for the delay before the expiration of the twenty-one (21) days. The Data User will be given an automatic extension of fourteen (14) days to fully comply with the DCR;

(b) request for supporting evidence from the Requestor before making any corrections under the DCR; and

(c) if Personal Data has been disclosed to a permitted Third Party (see Appendix IV) during the twelve (12) months immediately preceding the day on which the correction is made, the Data User will take practicable steps to supply the permitted Third Party with a copy of the corrected Personal Data together with a Written notice stating reason(s) for the correction. However, the Data User is not required to comply with such requirement if the disclosure of the Personal Data to a permitted Third Party consists of the permitted Third Party's own inspection of a register:

i. in which the Personal Data is entered or otherwise recorded; and

ii. which is available for inspection by the public.

7.4.4 DCR Limitations

The Data User is not required to correct or update Personal Data which is retained in order to comply with legal or other requirements to accurately reflect the reality in such cases for historical record-keeping (e.g. previous addresses retained for that purpose) and records of errors (e.g. the accurate recording of the event of the accidental termination of Data Subject's account).

7.4.5 Grounds for Refusal (Section 36 of the PDPA)

(a) The Data User has the right to refuse a DCR if:

i. the Data User is not supplied with necessary information as reasonably required to verify the identity of the Requestor; or if the DCR is requested by the Relevant Person, the identity of the Data Subject in relation to whom the Requestor claims to be the Relevant Person and that the Requestor is the Relevant Person in relation to the Data Subject;

Example (a1): *The Requestor submits the DCR form to correct the spelling error of the Data Subject's name such as from "Hamzah" to "Hamizah", but does not provide a copy of Official Identification Documents.*
Example (a2)*: The Requestor submits the DCR form to update the change of Data Subject's name, but does not provide certified true copy of Official Identification Documents of the Data Subject by the relevant authority to validate the information such as change of name due to conversion of religion.*

ii. the Data User is not supplied with such information as reasonably required to ascertain in what way the Personal Data to which the DCR relates is inaccurate, incomplete, misleading or not up-to-date;

iii. the Data User is not satisfied that the Personal Data to which the DCR relates is inaccurate, incomplete, misleading or not up-to-date;

iv. the Data User is not satisfied that the correction which is the subject of the DCR isaccurate, complete, not misleading or not up-to-date; or

v. any other data user controls the Processing of the Personal Data to which the DCR relates in such a way as to prohibit the first-mentioned Data User from complying, whether in whole or in part, with the DCR.

(b) the Data User must provide to the Requestor a Written notice of the refusal to comply together with reason(s) in the event the Data User is unable to comply with the DCR within twenty-one (21) days from the date of receipt of such DCR.

7.4.6 The Data User must maintain a record of all DCR received and the decisions made on each DCR. This will enable the Data User to answer any enquiry from the Requestor or investigations by the PDP Commissioner.

7.5 Right to Prevent Processing Likely to Cause Damage or Distress (Section 42 of the PDPA)

7.5.1 A Data Subject may request in Writing that the Data User ceases or does not begin the Processing of Personal Data. The Data Subject must justify why such Processing causes or is likely to cause "substantial and unwarranted damage or distress" to the Data Subject.

7.5.2 The PDPA does not define what is meant by "substantial damage or distress" and "unwarranted". However, in most cases:

(a) "substantial damage" includes financial loss or physical harm suffered by the Data Subject or another person;

(b) "substantial distress" includes emotional or mental pain suffered by the Data Subject or another person; and

(c) "unwarranted" means that the damage or distress suffered by the Data Subject or another person is not justifiable.

7.5.3 The Data Subject does not have the right to prevent Processing where:

(a) The Data Subject has consented to the Processing; or

(b) The Processing is necessary;

i. for the performance of a contract that the Data Subject has entered into;

ii. to take steps to enter into a contract at the request of the Data Subject;

iii. for the Data User to comply with any legal obligation to which the Data User is the subject, other than an obligation imposed by contract; or

iv. to protect the Data Subject's Vital Interests.

7.5.4 Upon receiving the Data Subject Notice, the Data User must, within twenty-one (21) days, provide the Data Subject with a Written notice:

(a) stating that the Data User has complied or intends to comply with the Data Subject Notice;

(b) if Data User does not intend to comply with the Data Subject Notice, to provide reasons for the decision; or

(c) stating reasons why the Data User finds the Data Subject Notice unjustified or to any extent unjustified and the extent to which the Data User has complied or intends to comply (if any).

7.5.5 In deciding 7.5.4 above, the Data User may consider the following before deciding to comply or not to comply with the Data Subject Notice:

(a) whether the Data Subject Notice has provided valid reason(s) that the Processing will cause "unwarranted" and "substantial damage or distress" to the Data Subject; and/or

(b) whether the damage or distress is substantial or unwarranted.
In the event the Data User believes that any damage or distress caused to the Data Subject is warranted or not substantial, the Data User may not comply with the Data Subject Notice. However, the Data User is required to provide the Data Subject with valid reason(s) for the refusal.

7.5.6 If the Data User decides not to comply with the Data Subject Notice, the Data Subject may submit an application to the PDP Commissioner to for the decision whether the Data User requires to comply with the Data Subject Notice.

7.5.7 The PDP Commissioner may require the Data User to comply with the Data Subject Notice, if the PDP Commissioner is satisfied that the Data Subject Notice is justified or justified to any extent. A Data User who fails to comply with the requirement of the PDP Commissioner commits an offence and shall, on conviction, be liable to a fine not exceeding RM200,000 or to imprisonment for a term not exceeding two (2) years or to both.

7.6 Right to Prevent Processing for Purposes of Direct Marketing (Section 43 of the PDPA)

7.6.1 Direct Marketing refers to the communication of advertising or marketing to specific individuals.

7.6.2 The Data User is permitted to conduct Direct Marketing to a Data Subject:

(a) if consent is obtained from the Data Subject;

(b) for the collection of Personal Data for sale of products or provision of services;

(c) if the Data Subject is informed of the identity of Direct Marketing organisations and the purpose of collection and disclosure;

(d) in the event the product and/or services offered to Data Subject are similar to the product and services generally provided by the Data User; or

(e) in the event the Data User is committed to providing an opt-out option for the Data Subject during the collection of the Personal Data.

7.6.3 However, marketing materials that are not directed at particular individuals but are instead sent to all consumers of the Data User or to an entire category/type of consumers of the Data User will not be considered as Direct Marketing for purposes of the PDPA and the CoP.

***Example (a)**: Marketing or promotional via SMS blasting or in electricity bills or invoices issued to all customers of a Data User is not considered as Direct Marketing.*
***Example (b)**: Directing promotional material to selected Data Subject with a record of prompt payment of electricity bills or invoices is considered as Direct Marketing.*

7.6.4 The Data User is not prevented from contacting a Data Subject for Direct Marketing, if the Data User provides an opt-out facility, to allow or not allow the use of Personal Data for Direct Marketing.

7.6.5 A Data Subject may at any time request in Writing to the Data User, require the Data User to cease or not to begin Processing his Personal Data for purposes of Direct Marketing, whereby the Data User must comply with such request within three (3) months from the receipt of the request.

7.6.6 If the Data Subject is dissatisfied with the failure of the Data User to comply in whole or in part with the Written request, the Data Subject may submit an application to the PDP Commissioner to require the Data User to comply. Failure by the Data User to comply with the requirement of the PDP Commissioner constitutes an offence liable to punishment with a fine not exceeding RM200,000 or to imprisonment for a term not exceeding two (2) years or both.

7.7 Right to Withdraw Consent to the Processing of Personal Data (Section 38 of the PDPA)

7.7.1 A Data Subject may by notice in Writing to the Data User withdraw the Data Subject's consent to the Processing of Personal Data.

7.7.2 However, the Data User may still process Personal Data if the withdrawal of consent would affect the Data User's rights and obligations, as set out below:

(a) for the performance of a contract to which the Data Subject is a party;

***Example (a1):** For the purpose of supplying or continuous supply of electricity by the Data User which requires the Processing of Data Subject's Personal Data, the Data Subject is not entitled to withdraw his consent as Processing of Personal Data is necessary for the performance of the contract.*
***Example (a2):** For the purpose to recover monies owed, Processing of Data Subject's Personal Data is necessary to give reminder to the Data Subject to issue demand letters or to commence legal proceeding against the Data Subject, as such, the Data Subject is not entitled to withdraw his consent as the recovery of monies by the Data User is part of the performance of the contract.*

(b) the right to be paid for services rendered, for example, the settlement of all electricity bills or tax invoices, overdue payments and cases on electricity theft;

(c) the right to bring and maintain legal proceedings against the Data Subject;

(d) the right to commence or continue with investigations involving the Data Subject;

(e) for legislation compliance and/or any non-contractual legal obligation;

(f) the obligation to maintain Personal Data for such durations as required under applicable legislation; for example, to retain Personal Data under the National Archive Act 2003; and

(g) the conduct of internal audits, risk management and/or fulfilment of legal or regulatory reporting requirements.

7.7.3 The Data User shall cease the Processing of the Personal Data upon receiving the notice in Writing. Failure of the Data User to cease the Processing of Personal Data constitutes an offence liable to punishment with a fine not exceeding RM100,000 or to imprisonment for a term not exceeding one (1) year or both.

8. GLOBAL DATA TRANSFER (SECTION 129 OF THE PDPA)

8.1 The Data User may not transfer Personal Data outside Malaysia unless the destination country is authorised by the Minister as published in the Gazette.

8.2 The Data User may transfer Personal Data outside Malaysia regardless of the above, if:

(a) the Data Subject has given consent to the transfer;

(b) the transfer is necessary to perform a contract between the Data User and the Data Subject;

(c) the transfer is necessary to perform another contract between the Data User and another party where the Data User has reasonable belief that the transfer is in the interests (e.g. rights, benefits, privileges, obligations or interests) of the Data Subject and it is not practicable to obtain consent in Writing, which would be likely to be provided in the event it was requested;

> ***Example (c)**: The Data User might typically transfer Personal Data outside of Malaysia to legal entities within the same group as the Data User (e.g. for the purpose of an overseas joint venture), or perhaps to overseas cloud data hosting vendors or locations.*

(d) the transfer is to comply with legal proceedings or to obtain legal advice;

(e) the Data User has reasonable grounds to believe:

i. the transfer is for the avoidance or mitigation of adverse action against the Data Subject;

ii. it is not practicable to obtain the consent in Writing of the Data Subject to that transfer; and

iii. the Data Subject would have given Data Subject's consent if it was practicable to obtain such consent;

(f) the Data User has taken all reasonable precautions (e.g. due diligence) to establish that the Personal Data will be treated in a manner which would be compliant with the PDPA;

> ***Example (f)**: Data User may transfer Personal Data outside of Malaysia if there is in that place in force any law which is substantially similar or equivalent to the level of protection afforded by the PDPA.*

(g) the transfer is necessary in order to protect the Vital Interests of Data Subject; or

(h) the transfer is in the public interest, as determined by the Minister.

8.3 The transfer of Personal Data via removable media device or cloud computing service is not permitted unless authorised in writing by an authorised officer of the Data User's top management.

8.4 The transfer of Personal Data via removable media device and cloud computing service should be recorded.

8.5 The transfer of Personal Data via cloud computing service must comply with the principles of Personal Data protection in Malaysia and other countries that have laws which is substantially similar to or that serves the same purposes as the PDPA.

8.6 The transfer of Personal Data via post, hand delivery, facsimile and other means should be recorded.

8.7 The transfer of Personal Data outside Malaysia in a prohibited manner constitutes an offence liable to a fine not exceeding RM300,000 or an imprisonment for a term not exceeding two (2) years or both as stipulated in Section 129 of the PDPA.

9. EMPLOYEES

9.1 Policies and Procedures

9.1.1 It is recommended that the Data User develops and implements policies and procedures specifying what should be done, what should not be done and standards expected of Employees in their day-to-day work when dealing with Personal Data.

9.1.2 In developing and implementing such policies and procedures, it is recommended that the Data User take the following points into consideration:

(a) the policies and procedures are to be communicated to the Data User's Employees;

(b) relevant Data User's Employees to be provided with training in relation to the policies and procedures, the PDPA, the PDP Regulations and the CoP;

(c) Employees' access to Data Subjects' Personal Data is to be restricted in accordance with its data access control policy and procedures;

(d) confidentiality clauses and possible sanctions against a breach are required to be built into the employment agreement or employment manual/handbook; and

(e) procedures in the event of a breach and appropriate action to be taken against an Employee responsible for the breach.

9.2 Training and Awareness

9.2.1 The Data User is required to implement appropriate training or awareness mechanisms for the relevant Data User's Employees to ensure that they understand the relevance of the policies and procedures to their roles and responsibilities.

9.2.2 Awareness program on relevant Personal Data policy and procedures should form part of every Data User's Employee's training.

9.3 Control Measures

9.3.1 The Data User is required to implement control measures to prevent the loss or compromise of the Personal Data in situations where policies and procedures are not followed by Employees.

9.3.2 An effective control measure should cover:

(a) Employees' access rights to Personal Data; and

(b) the implementation of security measures to prevent Personal Data breaches by the Employees.

9.3.3 In order to mitigate data security risks, Data User's Employees' access to Personal Data must be well controlled and Employees must only be provided with access to the Personal Data on a need to know basis. This includes, but not limited to the following:

(a) to terminate the access rights of the Employees to the Personal Data when the Employees leave the organisation, suspended, resign, retire, terminated, laid off or expiration of contract of employment;

(b) to provide a user ID and password for the Employees who are authorized to access the Personal Data; and

(c) to revoke/deactivate the user ID and password immediately when the Employees who are authorized to access personal data are no longer required to handle the Personal Data.

9.3.4 The Data User should control and limit the access rights of the Employees to the Personal Data for the purpose of collecting, Processing and storing of Personal Data.

9.3.5 The Data User must register and maintain a record of all Employees involved in the Processing of the Personal Data.

10. COMPLIANCE

10.1 Compliance

10.1.1 The Data User must develop and implement appropriate compliance policies, procedures and frameworks to ensure compliance with the PDPA and the CoP.

10.2 Monitoring

10.2.1 The Data User will monitor its compliance with the PDPA and the CoP by:

(a) implementing an internal monitoring framework; and

(b) conducting self-audits.

10.2.2 Upon identifying shortcomings and weaknesses in the implementation of the compliance framework, the Data User must ensure that appropriate remedial action is taken as soon as reasonably possible and the Data User shall resolve such shortcomings and weaknesses within ninety (90) days from the date it was discovered.

10.2.3 It is recommended that the Data User:

(a) implement a reporting system by key persons within the organisation (for example, the officer(s) responsible for Personal Data protection, heads of business units and relevant key Employees) to the senior management of the Data User, to review and assess the status of implementation of the PDPA and the CoP, to monitor issues, address shortcomings and track progress; and

(b) conduct periodic self-audits to identify issues in relation to compliance with the PDPA and the CoP.

10.2.4 The CoP shall be administered by all the Data Users in a forum.

10.2.5 The Data Users should meet with each other and if necessary, together with the PDP Commissioner at least once a year in order to discuss issues arising under the CoP and other related matters.

10.3 Amendment

10.3.1 The CoP may be amended, revised or updated to include all changes in the law. All such amendments, revisions or updates in the law will be notified to the Data User, in Writing, by the PDP Commissioner.

10.3.2 Amendments to the CoP may be made if:

(a) there are amendments to the PDPA or the PDP Regulations which will affect the implementation of the CoP;

(b) the PDP Commissioner makes amendments on his own accord; and/or

(c) the Data User make recommendations for amendments to the PDP Commissioner based on the results of the CoP review.

11. KEY CONTACTS

11.1 If you want to apply for a DAR, DCR or if you have any questions or comments regarding our data Processing activities relating to electricity supply, please contact:

Tenaga Nasional Berhad (TNB)	
Address	Tenaga Nasional Berhad, No 129, Jalan Bangsar, 59200, Kuala Lumpur.
Telephone	+603-2296 5566 (Headquarters) (8:00am to 5.15pm on business days). 1-300-88-5454 (One Stop Engagement Center - Billing Enquiries). 15454 (Call Management Centre – Outage Management).
Fax	+603-2283 3686.
Email	tnbcareline@tnb.com.my
Corporate Website	https://www.tnb.com.my
Sabah Electricity Sdn. Bhd. (SESB)	
Address	Wisma SESB, Jalan Tunku Abdul Rahman, 88673 Kota Kinabalu, Sabah, Malaysia.
Telephone	+6088-515000 and 15454 Customer Management Centre Department, Corporate Communication Division - (Technical Outage Management) – 24 hours - (Customer Services and Billing enquiries) – 8:00am to 5.15pm.
Fax	+6088-233582.
Email	crm@sesb.com.my
Corporate Website	https://www.sesb.com.my
Syarikat SESCO Berhad (SESCO)	
Address	Wisma SESCO, Jalan Bako, 93763 Petra Jaya, Kuching.
Telephone	1300-88-3111 (Customer Care Centre).
Fax	+6082-313588 (Technical and Billing enquiries). +6082-341063 (Corporate Information).
Email	customercare@sarawakenergy.com.my (Technical and billing enquiries). corpcomm@sarawakenergy.com.my (Corporate information).
Corporate Website	https://www.sarawakenergy.com.my

APPENDIX I

LIST OF OFFENCES AND PUNISHMENTS UNDER THE PERSONAL DATA PROTECTION ACT 2010 (ACT 709)

ITEM	SECTION/REGULATION	OFFENCE	PUNISHMENT
1	Subsection 5(2) Personal Data Protection Principle	Non-compliance with data Processing under Personal Data Protection Principle.	Fine not exceeding RM300,000 or imprisonment for a term not exceeding two (2) years or both.
2	Subsection 16(4) Certificate of registration	Process Personal Data without certificate of registration issued in 16(1)(a).	Fine not exceeding RM500,000 or imprisonment for a term not exceeding three (3) years or both.
3	Subsection 18(4) Revocation of registration	Process Personal Data after registration is revoked.	Fine not exceeding RM500,000 or imprisonment for a term not exceeding three (3) years or both.
4	Subsection 19(2) Surrender of certificate of registration	Failure to surrender the certificate of registration after it is revoked.	Fine not exceeding RM200,000 or imprisonment for a term not exceeding two (2) years or both.
5	Section 29 Non-compliance with the CoP	Non-compliance with any provision of the CoP that is applicable to the Data User.	Fine not exceeding RM100,000 or imprisonment for a term not exceeding one (1) year or both.
6	Section 37(4) Notification of refusal to comply with data correction request	Non-compliance with any provision in subsection 37(2).	Fine not exceeding RM100,000 or imprisonment for a term not exceeding one (1) year or both.
7	Subsection 38(4) Withdrawal of consent to process personal data	Continue to process Personal Data after withdrawal of consent by the Data Subject.	Fine not exceeding RM100,000 or imprisonment for a term not exceeding one (1) year or both.
8	Subsection 40(3) Processing of Sensitive Personal Data	Processing Sensitive Personal Data without complying with the conditions in subsection 40(1).	Fine not exceeding RM200,000 or imprisonment for a term not exceeding two (2) years or both.
9	Subsection 42(6) Right to prevent Processing likely to cause damage or distress	Non-compliance with the PDP Commissioner requirements in subsection 42(5).	Fine not exceeding RM200,000 or imprisonment for a term not exceeding two (2) years or both.

10	Subsection 43(4) Right to prevent Processing for the purpose of Direct Marketing	Non-compliance with the PDP Commissioner requirements in subsection 43(3).	Fine not exceeding RM200,000 or imprisonment for a term not exceeding two (2) years or both.
11	Subsection 108(8) Enforcement notice	Non-compliance with an enforcement notice.	Fine not exceeding RM200,000 or imprisonment for a term not exceeding two (2) years or both.
12	Subsection 113(7) Search and seizure with warrant	A person who without lawful authority, breaks, tampers with or damages the seal referred to in subsection 113(6) or removes any computer, book, account, computerised data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article under seal or attempts to do so.	Fine not exceeding RM50,000 or imprisonment for a term not exceeding six (6) months or both.
13	Section 120 Obstruction to search	Any person who- (a) Refuses to give access to any authorised officer; (b) Assaults, obstructs, hinders or delays any authorised officer; or (c) Refuses any authorised officer any information relating to an offence or suspected offence.	Imprisonment for a term not exceeding two (2) years or fine not exceeding RM10,000 or both.
14	Subsection 129(5) Transfer of personal data to places outside Malaysia	Non-compliance with requirements in subsection 129(1) – transfer Personal Data of a Data Subject to a place outside Malaysia unless to such a place as specified by the Minister, upon the recommendation of PDP Commissioner, by notification published in the Gazette.	Fine not exceeding RM300,000 or imprisonment for a term not exceeding two (2) years or both.

15	Subsection 130(7) Unlawful collecting, etc., of Personal Data	Committing offences as prescribed in Section 130.	Fine not exceeding RM500,000 or imprisonment for a term not exceeding three (3) years or both.
16	Subsection 131(1) and (2) Abetment and attempt punishable as offences	131(1) Abetment of a commission of or attempts to commit any offence under the PDPA.	Provided that any term of imprisonment shall not exceed half of the maximum term provided for the offence under the PDPA.
		131(2) Commission of any act preparatory to or in furtherance of the commission of any offence under the PDPA.	Provided that any term of imprisonment shall not exceed half of the maximum term provided for the offence under the PDPA.
17	141(2) Obligation of secrecy	Offence under 141(1) (a) and (b) - the Commissioner, its officer or servant, any member of the Advisory Committee, any member, officer or servant of the Appeal Tribunal, any authorized officer or any person attending any meeting or deliberation of the Advisory Committee, whether during or after his tenure of office or employment, at any time shall not Disclose any information obtained by him in the course of his duties.	Fine not exceeding RM100,000 or imprisonment for a term not exceeding one (1) year or both.
18	Subsection 143(3) Power to make regulation	Non-compliance with any regulation or any other subsidiary legislation under this section.	Penalties of a fine not exceeding RM250,000 or imprisonment for a term not exceeding two (2) years or both.

PERSONAL DATA PROTECTION REGULATION 2013			
1	Regulation 12 Penalty	Non-compliance with the following: Subregulation 3(1) Consent of Data Subject. Subregulation 6 Security policy. Subregulation 7 Retention standard. Subregulation 8 Data integrity standard.	Penalties of a fine not exceeding RM250,000 or imprisonment for a term not exceeding two (2) years or both.
PERSONAL DATA PROTECTION (REGISTRATION OF DATA USER) REGULATIONS 2013			
1	Regulation 5 Renewal of certificate of registration	Failure to renew certificate of registration.	Penalties of a fine not exceeding RM250,000 or imprisonment for a term not exceeding two (2) years or both.
2	Regulation 6 Change of particulars in certificate of registration	Failure to notify the commissioner of any change to the particulars of certificate of registration.	Penalties of a fine not exceeding RM250,000 or imprisonment for a term not exceeding two (2) years or both.
3	Regulation 8 Display of certificate of registration and other information	Failure to display certificate of registration and other information.	Penalties of a fine not exceeding RM10,000 or imprisonment for a term not exceeding one (1) year or both.

APPENDIX II

[This template DAR form is for reference purpose only. The Data Users may revise/ amend the template according to their own business needs and where applicable].

PERSONAL DATA ACCESS REQUEST ("DAR") FORM
BORANG PERMINTAAN MENGAKSES DATA PERIBADI ("PMD")

[Section 30(2) of Personal Data Protection Act 2010 ("PDPA")]
[Seksyen 30(2) Akta Perlindungan Data Peribadi 2010 ("APDP")]

Data User will process this DAR within 21 days from the date of receipt of the completed DAR form together with supporting document(s) and/or relevant information, with an extension of 14 days, if necessary.
Pengguna Data akan memproses PMD ini dalam masa 21 hari dari tarikh penerimaan borang PMD yang lengkap beserta dokumen sokongan dan/atau maklumat yang relevan, dengan tempoh lanjutan 14 hari, jika perlu.

PERSONAL DATA ACCESS REQUEST/ *PERMINTAAN AKSES DATA PERIBADI*

Please tick [✓] the appropriate box/*Sila tandakan [✓] pada petak yang sesuai:*

[ ] I am a customer/ former customer of the data user and I would like to access my personal data (Please proceed to **Part 1** of this form).
*Saya merupakan/ pernah menjadi pelanggan pengguna data dan saya ingin mengakses data peribadi saya (Sila teruskan ke **Bahagian 1** borang ini).*

[ ] I am making a request for personal data on behalf of the data subject (Please proceed to **Part 2** of this form).
*Saya membuat permintaan untuk data peribadi bagi pihak subjek data (Sila teruskan ke **Bahagian 2** borang ini).*

Please refer to the last part of this form (Important Notice to the Requestor) before proceeding with this DAR.
Sila rujuk bahagian akhir borang ini (Nota Penting kepada Peminta) sebelum meneruskan dengan PMD ini.

PART 1: DATA SUBJECT/ *SUBJEK DATA* **(all fields are mandatory to be completed/ *semua ruangan perlu dilengkapkan*)**		
Name/ *Nama*	:	
Identity Card Number or Passport Number *Nombor Kad Pengenalan atau Nombor Pasport*	:	
Correspondence Address *Alamat Surat-Menyurat*	:	
Telephone Number (Mobile/Office/House)* *Nombor Telefon (Telefon bimbit/Pejabat/Rumah)**	:	
Email Address (if any)/*Alamat Emel(jika ada)*	:	
Account Number/ *Nombor Akaun**	:	

*delete if not applicable/*potong jika tidak berkenaan*

PART 2: RELEVANT PERSON/ *ORANG YANG BERKAITAN*
(all fields are mandatory to be completed/ ***semua ruangan perlu dilengkapkan)***

My request is based on the following:
Permintaan saya adalah berdasarkan yang berikut:

[ ] Data subject's authorisation/power of attorney
Kebenaran/surat kuasa wakil dari subjek data
[ ] Data subject's legal/personal representative/executor/administrator
Wakil di sisi undang-undang/wakil diri subjek data/wasi/pentadbir harta pusaka
[ ] Warrant/ court order
Waran/ perintah mahkamah
[ ] Others (please specify): _____
Lain-lain (sila nyatakan)

A. PARTICULARS OF DATA SUBJECT/ *BUTIRAN SUBJEK DATA*

Name/ *Nama*	:	
Identity Card Number or Passport Number *Nombor Kad Pengenalan atau Nombor Pasport*	:	
Account Number/ *Nombor Akaun**	:	

B. PARTICULARS OF RELEVANT PERSON/ *BUTIRAN ORANG YANG BERKAITAN*

Name/ *Nama*	:	
Identity Card Number or Passport Number *Nombor Kad Pengenalan atau Nombor Pasport*	:	
Correspondence Address *Alamat Surat-Menyurat*	:	
Telephone Number (Mobile/Office/House*) *Nombor Telefon (Telefon bimbit/Pejabat/Rumah*)*	:	
Email Address (if any)/*Alamat Emel (jika ada)*	:	

PART 3: DESCRIPTION OF PERSONAL DATA REQUESTED
PENERANGAN MENGENAI DATA PERIBADI YANG DIMINTA

For data subject only – Please tick [✓] if agree to access and authorize TNB to send the monthly electricity bill via the email address mentioned in Part 1/ ***Bagi subjek data sahaja*** *– Sila tandakan [✓] jika bersetuju untuk mengakses dan membenarkan TNB untuk menghantar bil elektrik bulanan melalui alamat emel yang dinyatakan dalam Bahagian 1.*

*delete if not applicable/*potong jika tidak berkenaan*

PART 4: DETAILS OF REQUEST/ *PERINCIAN PERMINTAAN*

Please tick [✓] the appropriate box/*Sila tandakan [✓] pada petak yang sesuai:*

I hereby request the following/ *Saya dengan ini meminta yang berikut:*

1. A copy of personal data:
   Salinan maklumat data peribadi:

   [ ] Yes
   Ya

   [ ] No
   Tidak

2. Mode of communication:
   Cara komunikasi:

   [ ] normal post;
   pos biasa;
   [ ] email; or
   emel; or
   [ ] self-collect at the branch where the DAR is made.
   pengambilan sendiri di cawangan di mana PMD itu dibuat.

PART 5: UNDERTAKING BY REQUESTOR/*AKUJANJI PEMINTA*

1. I/We hereby certify that the information given in this form and any document(s) submitted are true and accurate.
   Saya/Kami dengan ini mengesahkan bahawa maklumat yang diberikan dalam borang ini dan mana-mana dokumen yang dimajukan adalah benar dan tepat.

2. I/We understand that:
   Saya/Kami memahami bahawa:
   i. It will be necessary for the data user to verify my/our identity(ies);
      Pengguna data perlu mengesahkan identiti saya/kami;
   ii. The data user may contact me/us for more detailed information regarding this DAR; and
      Pengguna data boleh menghubungi saya/kami untuk maklumat yang lebih terperinci berkenaan PMD ini; dan
   iii. All personal data provided by me/us in this form will be collected and processed by the data user as personal data in accordance with the PDPA.
      Semua data peribadi yang diberikan oleh saya/kami dalam borang ini akan dikumpulkan dan diproses oleh pengguna data sebagai data peribadi menurut APDP.

3. I/We hereby agreed to indemnify the data user for any losses, costs and expenses incurred by the data user in connection with this DAR or in the event that any information and/or document(s) submitted by me/us is/are not true.
   Saya/Kami dengan ini bersetuju untuk menanggung rugi sebarang kerugian, kos dan perbelanjaan, yang ditanggung oleh pengguna data berkaitan dengan PMD ini atau sekiranya apa-apa maklumat dan/atau dokumen yang diserahkan oleh saya/kami adalah tidak benar.

4. [Applicable to relevant person only] I/We hereby confirm that consent from the data subject has been obtained for this DAR and below is the true signature of data subject (where applicable).
   [Terpakai kepada orang yang berkaitan sahaja] Saya/Kami dengan ini mengesahkan bahawa persetujuan subjek data telah diperolehi untuk PMD ini dan di bawah adalah tandatangan sebenar subjek data (di mana berkenaan).

.....	.....
(Signature of data subject)*	(Signature of relevant person)*
(Tandatangan subjek data)	*(Tandatangan orang yang berkaitan)*
Date:	Date:
Tarikh	*Tarikh*

*delete if not applicable/*potong jika tidak berkenaan*

NOTIFICATION BY DATA USER/ *PEMAKLUMAN OLEH PENGGUNA DATA*

ACCESS GRANTED
AKSES DIBERI

☐ Yes, within 21 days with/ without* an extension of 14 days.
Ya, dalam tempoh masa 21 hari dengan/ tanpa tempoh lanjutan 14 hari.*

(Reason for extension of 14 days/ *Sebab lanjutan tempoh masa 14 hari)*

☐ No.
Tidak.

Reason for refusal by data user/ *Sebab penolakan oleh pengguna data:*

Please tick [✓] the appropriate box/*Sila tandakan [✓] pada petak yang sesuai:*

	a. Insufficient information. *Maklumat tidak mencukupi.*
	b. Request involves disclosure of personal data relating to other individuals. *Permintaan melibatkan penzahiran data peribadi individu lain.*
	c. Failure to provide identity verification of the requestor. *Gagal mengemukakan pengesahan identiti oleh peminta.*
	d. Other data user(s) control the processing of personal data. *Pemprosesan data peribadi dikawal oleh pengguna data yang lain.*
	e. Involves high cost and risk for the data user. *Melibatkan kos dan risiko yang tinggi di pihak pengguna data.*
	f. Violation of a court order. *Melanggar perintah mahkamah.*
	g. Disclosure involves confidential commercial information. *Penzahiran melibatkan maklumat komersial yang sulit.*

FOR DATA USER USE ONLY/ *UNTUK KEGUNAAN PENGGUNA DATA SAHAJA*

Date of receipt: _____
Tarikh penerimaan

Processed by:
Diproses oleh

Date of completion: _____
Tarikh selesai

.....
Name:
Nama
Designation:
Jawatan

*delete if not applicable/*potong jika tidak berkenaan*

IMPORTANT NOTICE TO THE REQUESTOR/ *NOTA PENTING KEPADA PEMINTA*

This DAR can be made to the data user by:
PMD ini boleh dibuat kepada pengguna data oleh:

a. A Data subject; or
Subjek data; atau
b. Relevant person (on behalf of the data subject) who is:
Orang yang berkaitan (bagi pihak subjek data) yang merupakan:
i. A parent/legal guardian/legal representative of the data subject (who is below the age of 18);
Ibu bapa/penjaga/wakil di sisi undang-undang subjek data (yang berumur di bawah 18 tahun);
ii. A person appointed by the court to manage the data subject's affairs; or
Orang yang dilantik oleh mahkamah untuk menguruskan urusan subjek data; atau
iii. A person/ an entity acting under the data subject's authorisation/power of attorney to make this DAR on behalf of the data subject.
Mana-mana orang/entiti yang bertindak di bawah pemberian kuasa/surat kuasa wakil untuk membuat PMD ini bagi pihak subjek data.

Supporting Documents Required/ *Dokumen-Dokumen Sokongan Yang Diperlukan*

a. If the DAR is requested by the **data subject**:
Sekiranya PMD dibuat oleh subjek data:

i. A copy of the data subject's Identity Card (IC) e.g. MyKad, MyPR, MyKAS, MyTentera; or Passport bearing signature of the data subject; or other certified documentary proof of identity.
Satu salinan Kad Pengenalan (KP) subjek data sebagai contoh, MyKad, MyPR, MyKAS, MyTentera; atau Pasport yang mengandungi tanda tangan subjek data; atau lain-lain bukti pengenalan diri dokumentar yang diperakui.

b. If the DAR is requested by the **relevant person**:
Sekiranya PMD dibuat oleh orang yang berkaitan:

i. A copy of the relevant person's Identity Card (IC) e.g. MyKad, MyPR, MyKAS, MyTentera; or Passport bearing signature of relevant person; or other certified documentary proof of identity (data subject's proof of identity is not required); and
Satu salinan Kad Pengenalan (KP) orang yang berkaitan sebagai contoh, MyKad, MyPR, MyKAS, MyTentera; atau Pasport yang mengandungi tanda tangan orang yang berkaitan; atau lain-lain bukti pengenalan diri dokumentar yang diperakui (bukti pengenalan diri subjek data tidak diperlukan); dan

ii. Any document evidencing the right/authority of the relevant person to the information of the data subject such as an authorisation letter, warrant, court order or power of attorney. The authorisation letter from the data subject is not required if the data subject signs Part 5 (Undertaking) of this form.
Sebarang dokumen yang membuktikan hak/kuasa orang yang berkaitan kepada maklumat subjek data, seperti surat pemberian kuasa, waran, perintah mahkamah atau surat kuasa wakil. Surat pemberian kuasa dari subjek data tidak diperlukan jika subjek data menandatangani Bahagian 5 (Akujanji) borang ini.

Processing Fee/ *Fi Pemprosesan*

Processing fee may be charged as per table below:
Fi pemprosesan boleh dikenakan seperti jadual di bawah:

Item *Bil.*	Type of DAR *Jenis-jenis PMD*	Fees (RM) *Fi (RM)*
1	DAR for the data subject's personal data with a copy *PMD untuk data peribadi subjek data berserta salinan*	10
2	DAR for the data subject's personal data without a copy *PMD untuk data peribadi subjek data tanpa salinan*	2
3	DAR for the data subject's sensitive personal data with a copy *PMD untuk data peribadi sensitif subjek data berserta salinan*	30
4	DAR for the data subject's sensitive personal data without a copy *PMD untuk data peribadi sensitif subjek data tanpa salinan*	5

Note: If Sales and Service Tax (SST)/Goods and Services Tax (GST) is imposed on the fee, data subject will pay for all SST/GST.
Nota: Jika Cukai Jualan dan Perkhidmatan (SST)/Cukai Barangan dan Perkhidmatan (GST) dikenakan ke atas fi, subjek data akan membayar kesemua SST/GST.

APPENDIX III

[This template DCR form is for reference purpose only. The Data Users may revise/ amend the template according to their own business needs and where applicable].

PERSONAL DATA CORRECTION REQUEST ("DCR") FORM
BORANG PERMINTAAN PEMBETULAN DATA PERIBADI ("PPD")

[Section 34(1) of Personal Data Protection Act 2010 ("PDPA")]
[Seksyen 34(1) Akta Perlindungan Data Peribadi 2010 ("APDP")]

Data User will process this DCR within 21 days from the date of receipt of the completed DCR form together with supporting document(s) and/or relevant information, with an extension of 14 days, if necessary.
Pengguna Data akan memproses PPD ini dalam masa 21 hari dari tarikh penerimaan borang PPD yang lengkap beserta dokumen sokongan dan/atau maklumat yang relevan, dengan tempoh lanjutan 14 hari, jika perlu.

PERSONAL DATA CORRECTION REQUEST/ *PERMINTAAN PEMBETULAN DATA PERIBADI*

Please tick [✓] the appropriate box/ *Sila tandakan [✓] pada petak yang sesuai:*

[ ] I am a customer/ former customer of the data user and I would like to correct my personal data (Please proceed to **Part 1** of this form).
*Saya merupakan/ pernah menjadi pelanggan pengguna data dan saya ingin membetulkan data peribadi saya (Sila teruskan ke **Bahagian 1** borang ini).*

[ ] I am making a request for correction of personal data on behalf of the data subject (Please proceed to **Part 2** of this form).
*Saya membuat permintaan untuk membetulkan data peribadi bagi pihak subjek data (Sila teruskan ke **Bahagian 2** borang ini).*

Please refer to the last part of this form (Important Notice to the Requestor) before proceeding with this DCR.
Sila rujuk bahagian akhir borang ini (Nota Penting kepada Peminta) sebelum meneruskan dengan PPD ini.

PART 1: DATA SUBJECT/ *SUBJEK DATA* **(all fields are mandatory to be completed/ *semua ruangan perlu dilengkapkan*)**		
Name/ *Nama*	:	
Identity Card Number or Passport Number *Nombor Kad Pengenalan atau Nombor Pasport*	:	
Correspondence Address *Alamat Surat-Menyurat*	:	
Telephone Number (Mobile/Office/House)* *Nombor Telefon (Telefon bimbit/Pejabat/Rumah)**	:	
Email Address (if any)/*Alamat Emel(jika ada)*	:	
Account Number/ *Nombor Akaun**	:	

*delete if not applicable/*potong jika tidak berkenaan*

PART 2: RELEVANT PERSON/ *ORANG YANG BERKAITAN*
(all fields are mandatory to be completed/*semua ruangan perlu dilengkapkan)*

My request is based on the following:
Permintaan saya adalah berdasarkan yang berikut:

[ ] Data subject's authorisation/power of attorney
Kebenaran/surat kuasa wakil dari subjek data
[ ] Data subject's legal/personal representative/executor/administrator
Wakil di sisi undang-undang/wakil diri subjek data/wasi/pentadbir harta pusaka
[ ] Warrant/ court order
Waran/ perintah mahkamah
[ ] Others (please specify): _____
Lain-lain (sila nyatakan)

A. PARTICULARS OF DATA SUBJECT/ *BUTIRAN SUBJEK DATA*

Name/ *Nama*	:	
Identity Card Number or Passport Number *Nombor Kad Pengenalan atau Nombor Pasport*	:	
Account Number/ *Nombor Akaun**	:	

B. PARTICULARS OF RELEVANT PERSON/ *BUTIRAN ORANG YANG BERKAITAN*

Name/ *Nama*	:	
Identity Card Number or Passport Number *Nombor Kad Pengenalan atau Nombor Pasport*	:	
Correspondence Address *Alamat Surat-Menyurat*	:	
Telephone Number (Mobile/Office/House*) *Nombor Telefon (Telefon bimbit/Pejabat/Rumah*)*	:	
Email Address (if any)/*Alamat Emel (jika ada)*	:	

PART 3: CORRECTION OF DATA SUBJECT'S PERSONAL DATA
PEMBETULAN DATA PERIBADI SUBJEK DATA

a. Details of Personal Data *Butiran Data Peribadi*	b. Before Correction *Sebelum Pembetulan*	c. After Correction *Selepas Pembetulan*

*delete if not applicable/*potong jika tidak berkenaan*

PART 4: NOTIFICATION OF CORRECTED PERSONAL DATA
PEMAKLUMAN BAGI DATA PERIBADI YANG TELAH DIBETULKAN

Please tick [☑] the appropriate box/*Sila tandakan [☑] pada petak yang sesuai:*

a. Mode of communication:
Cara komunikasi:

[ ] normal post;
pos biasa;
[ ] email; or
emel; atau
[ ] self-collect at the branch where the DCR is made.
pengambilan sendiri di cawangan di mana PPD itu dibuat.

PART 5: UNDERTAKING BY REQUESTOR/*AKUJANJI PEMINTA*

1. I/We hereby certify that the information given in this form and any document(s) submitted are true and accurate.
Saya/Kami dengan ini mengesahkan bahawa maklumat yang diberikan dalam borang ini dan mana-mana dokumen yang dimajukan adalah benar dan tepat.

2. I/We understand that:
Saya/Kami memahami bahawa:
   i. It will be necessary for the data user to verify my/our identity(ies);
   Pengguna data perlu mengesahkan identiti saya/kami;
   ii. The data user may contact me/us for more detailed information regarding this DCR; and
   Pengguna data boleh menghubungi saya/kami untuk maklumat yang lebih terperinci berkenaan PPD ini; dan
   iii. All personal data provided by me/us in this form will be collected and processed by the data user as personal data in accordance with the PDPA.
   Semua data peribadi yang diberikan oleh saya/kami dalam borang ini akan dikumpulkan dan diproses oleh pengguna data sebagai data peribadi menurut APDP.

3. I/We hereby agreed to indemnify the data user for any losses, costs and expenses incurred by the data user in connection with this DCR or in the event that any information and/or document(s) submitted by me/us is/are not true.
Saya/Kami dengan ini bersetuju untuk menanggung rugi sebarang kerugian, kos dan perbelanjaan, yang ditanggung oleh pengguna data berkaitan dengan PPD ini atau sekiranya apa-apa maklumat dan/atau dokumen yang diserahkan oleh saya/kami adalah tidak benar.

4. [Applicable to relevant person only] I/We hereby confirm that consent from the data subject has been obtained for this DCR and below is the true signature of data subject (where applicable).
[Terpakai kepada orang yang berkaitan sahaja] Saya/Kami dengan ini mengesahkan bahawa persetujuan subjek data telah diperolehi untuk PPD ini dan di bawah adalah tandatangan sebenar subjek data (di mana berkenaan).

.....	.....
(Signature of data subject)*	(Signature of relevant person)*
(Tandatangan subjek data)	*(Tandatangan orang yang berkaitan)*
Date:	Date:
Tarikh	*Tarikh*

*delete if not applicable/*potong jika tidak berkenaan*

NOTIFICATION BY DATA USER/ *PEMAKLUMAN OLEH PENGGUNA DATA*

PERSONAL DATA CORRECTION
PEMBETULAN DATA PERIBADI

☐ Yes, within 21 days with/ without* an extension of 14 days.
Ya, dalam tempoh masa 21 hari dengan/ tanpa tempoh lanjutan 14 hari.*

_____
(Reason for extension of 14 days/ *Sebab lanjutan tempoh masa 14 hari)*

☐ No.
Tidak.

Reason for refusal by data user/ *Sebab penolakan oleh pengguna data:*

Please tick [✓] the appropriate box/*Sila tandakan [✓] pada petak yang sesuai:*

	a. Failure to provide identification verification of the requestor. *Kegagalan mengemukakan pengesahan identiti oleh peminta.*
	b. Data user is satisfied that the existing personal data is accurate, complete, not misleading or up-to-date. *Pengguna data berpuas hati bahawa data peribadi sedia ada adalah tepat, lengkap, tidak mengelirukan atau terkini.*
	c. Insufficient information to ascertain in what way the personal data is inaccurate, incomplete, misleading or not up-to-date. *Maklumat tidak mencukupi untuk menentukan bagaimana data peribadi itu yang dengannya permintaan pembetulan data itu adalah kurang tepat, tidak lengkap, mengelirukan atau tidak terkini.*
	d. Other data user controls the processing of the personal data. *Pengguna data lain mengawal pemprosesan data peribadi.*
	e. Data user is satisfied that the expression of opinion is accurate, complete, not misleading or up-to-date. *Pengguna data berpuas hati bahawa penyataan pendapat adalah tepat, lengkap, tidak mengelirukan atau terkini.* Note from data user (mandatory to specify the reason) *Catatan daripada pengguna data (wajib nyatakan sebab)* _____ _____

FOR DATA USER USE ONLY/ *UNTUK KEGUNAAN PENGGUNA DATA SAHAJA*

Date of receipt: _____
Tarikh penerimaan

Date of completion: _____
Tarikh selesai

Processed by:
Diproses oleh

.....
Name:
Nama
Designation:
Jawatan

*delete if not applicable/*potong jika tidak berkenaan*

IMPORTANT NOTICE TO THE REQUESTOR/ *NOTA PENTING KEPADA PEMINTA*

This DCR can be made to the data user by:
PPD ini boleh dibuat kepada pengguna data oleh:

a. A Data subject; or
Subjek data; atau
b. Relevant person (on behalf of the data subject) who is:
Orang yang berkaitan (bagi pihak subjek data) yang merupakan:
   i. A parent/legal guardian/legal representative of the data subject (who is below the age of 18);
   Ibu bapa/penjaga/wakil di sisi undang-undang subjek data (yang berumur di bawah 18 tahun);
   ii. A person appointed by the court to manage the data subject's affairs; or
   Orang yang dilantik oleh mahkamah untuk menguruskan urusan subjek data; atau
   iii. A person/ an entity acting under the data subject's authorisation/power of attorney to make this DCR on behalf of the data subject.
   Mana-mana orang/entiti yang bertindak di bawah pemberian kuasa/surat kuasa wakil untuk membuat PPD ini bagi pihak subjek data.

Supporting Documents Required/ *Dokumen-Dokumen Sokongan Yang Diperlukan*

a. If the DCR is requested by the **data subject**:
Sekiranya PPD dibuat oleh subjek data:

   i. A copy of the data subject's Identity Card (IC) e.g. MyKad, MyPR, MyKAS, MyTentera; or Passport bearing signature of the data subject; or other certified documentary proof of identity; and
   Satu salinan Kad Pengenalan (KP) subjek data sebagai contoh, MyKad, MyPR, MyKAS, MyTentera; atau Pasport yang mengandungi tanda tangan subjek data; atau lain-lain bukti pengenalan diri dokumentar yang diperakui; dan

   ii. Any supporting documents relating to this request.
   Sebarang dokumen sokongan berkenaan permintaan ini.

b. If the DCR is requested by the **relevant person**:
Sekiranya PMD dibuat oleh orang yang berkaitan:

   i. A copy of the relevant person's Identification Card ("IC") e.g. MyKad, MyPR, MyKAS, MyTentera; or Passport bearing signature of relevant person; or other certified documentary proof of identity (data subject's proof of identity is not required);
   Satu salinan Kad Pengenalan ("KP") orang yang berkaitan sebagai contoh, MyKad, MyPR, MyKAS, MyTentera; atau Pasport yang mengandungi tanda tangan orang yang berkaitan; atau lain-lain bukti pengenalan diri dokumentar yang diperakui (bukti pengenalan diri subjek data tidak diperlukan);

   ii. Any document evidencing the right/authority of the relevant person to correct the data subject's information such as an authorisation letter, warrant, court order or power of attorney. The authorisation letter from the data subject is not required if the data subject signs Part 5 (Undertaking) of this form; and
   Sebarang dokumen yang membuktikan hak/kuasa orang yang berkaitan untuk membetulkan maklumat subjek data, seperti surat pemberian kuasa, waran, perintah mahkamah atau surat kuasa wakil. Surat pemberian kuasa dari subjek data tidak diperlukan jika subjek data menandatangani Bahagian 5 (Akujanji) borang ini; dan

   iii. Any supporting documents relating to this request.
   Sebarang dokumen sokongan berkenaan permintaan ini.

Processing Fee/ *Fi Pemprosesan*

Fee is not imposed to this DCR.
Fi tidak dikenakan ke atas PPD ini.

APPENDIX IV

LIST OF PERMITTED THIRD PARTIES FOR DISCLOSURE
[Section 8(b) of the Personal Data Protection Act 2010]

(This Appendix is not intended to be exhaustive but may be amended from time to time by the Data User as required by business needs.)

NO.	PERMITTED THIRD PARTIES
1.	The industry regulator where the Data User has legal obligation towards it as follows: ▪ Energy Commission of Malaysia for TNB and SESB ▪ Director of Electricity Supply for Sarawak for SESCO.
2.	Federal Government, State Government, a local authority, a statutory authority exercising powers vested in it by federal or state law but subject to conditions as stipulated in clause 6.1.4 of the CoP.
3.	Where Data User is required or authorised by any court order/ tribunal or authority whether government or quasi government with jurisdiction over the Data User.
4.	Approved bodies where Employees contributions are remitted: ▪ Social Security Organisation (SOCSO) ▪ Baitulmal ▪ Pusat Zakat ▪ Lembaga Tabung Haji ▪ Yayasan Pembangunan Ekonomi Islam Malaysia (YaPEIM) ▪ Employees Provident Fund (EPF) ▪ Koperasi ▪ Insurer.
5.	Immediate family members of Data Subject to protect the Vital Interests of the Data Subject and/or for purpose of obtaining current electricity bill only with proof of relationship or authorisation letter: ▪ Father ▪ Mother ▪ Husband ▪ Wife ▪ Children ▪ Siblings.

6.	Tenant and/or owner of the premises where the electricity is supplied (whom is not a registered consumer) for purpose of obtaining current electricity bill only (with supporting documents or authorisation letter).
7.	Financial institutions, merchants, VISA International Services Association, MasterCard International Incorporated and other card associations (in relation to credit cards issue to Data Subject) for the purpose of payment of electricity bill or other services of the Data User.
8.	Any person intending to settle the outstanding amount in relation to the Data User services to Data Subject.
9.	Any credit reporting agency.
10.	Any successful bidder or his lawyer for the purpose of payment electricity bill under the proclamation of sale.
11.	Doctors/ clinics/ hospitals/ pharmacists to protect the Vital Interests of Data Subject.
12.	Subsidiaries of the Data User.
13.	To the parties that the Data User may transfer rights and obligations pursuant to the agreement endorsed with Data Subject.

DATA PROTECTION OFFICER
LEGAL SERVICES DEPARTMENT
TENAGA NASIONAL BERHAD

Email: dpo@tnb.com.my

First Edition (Version 2.0) 2020