PETRONAS

Master Guidelines to the PETRONAS Corporate Privacy Policy

Contents

Section 6: Transferring Personal Data to Different Countries

Section 7: Data Subject Rights

Section 8: Personal Data Breaches

Section 9: Communications with Customers and Stakeholders

Section 10: Employee Personal Data

Section 11: Biometric Data

Section 1: Introduction

This Master Guidelines to PETRONAS Corporate Privacy Policy ("Guidelines") is an operational document intended to complement the PETRONAS Corporate Privacy Policy ("Corporate Privacy Policy") and is intended to apply in all countries in which PETRONAS Group conducts its business.

The Guideline Principles take into account the core principles in the Corporate Privacy Policy and best practices based on the personal data protection and privacy laws of relevant jurisdictions.

These Guidelines provide an overview of the principles that apply within PETRONAS Group for processing of personal data about any individuals (whether personal data of customers, employees, suppliers, service providers, business partners, etc.) which includes collecting, storing, transferring, etc. ("Guideline Principles").

1.0 Objective

1.0.1 The purpose of these Guidelines is to support PETRONAS' goal of ensuring that the flow of Personal Data PETRONAS manages everyday is processed safely, respecting individual rights to data protection and privacy, and in compliance with applicable personal data protection and privacy laws. These Guidelines are therefore intended to serve as high level guidance, subject to applicable personal data protection laws of the jurisdiction on how to determine whether Personal Data is involved, and which requirements need to be complied with in that case.

1.0.2 As this is a high-level guideline, it is necessary to take into account and comply with any specific requirements of the **local personal data protection and privacy laws** of the respective jurisdictions of the relevant PETRONAS entity, **as well as any internal guidelines and processes issued in accordance with those laws**.

1.0.3 These Guideline Principles should be followed and practised in the everyday processing of Personal Data in PETRONAS Group, which are briefly summarised in the following applicable situations/scenarios:

i. in identifying Personal Data – see Section 3;

ii. when collecting Personal Data – see Section 4;

iii. when managing and controlling Personal Data – see Section 5;

iv. when transferring Personal Data to different countries – see Section 6;

v. when handling enquiries and responding to requests from individuals regarding their Personal Data – see Section 7;

vi. when security incidents occur that may lead to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data – see Section 8;

vii. when managing communications with customers and stakeholders – see Section 9;

viii. when handling personal data in the context of human resources – see Section 10; and

ix. when processing biometric data – see Section 11.

1.0.4 You may refer to **Appendix I – Master Guidelines Checklist**, which provides a general guide to assessing personal data protection and privacy compliance in accordance with these Guidelines.

1.0.5 PETRONAS may review and modify these Guidelines from time to time in compliance with the requirements of applicable law.

1.1 Scope of Application

1.1.1 These Guidelines are intended to apply to PETRONAS Group, including its employees, officers and directors.

1.1.2 It is the responsibility of all employees, officers or directors of the PETRONAS Group to read, understand and comply with these Guidelines. Failure to comply may have severe consequences for PETRONAS or PETRONAS Group and may result in consequence management pursuant to COBE.

1.1.3 Joint venture companies in which PETRONAS Group is a non-controlling co-venturer and associated companies are encouraged to adopt these Guidelines or similar principles and standards.

1.1.4 PETRONAS further encourages its contractors, subcontractors, consultants, agents, representatives and others performing work or services for or on behalf of PETRONAS Group to comply with the relevant sections of these Guidelines when performing their work or services. Failure to comply with the principles and standards set out in these Guidelines may cause non-compliance with relevant personal data protection legislation, resulting in the termination of the non-complying party's relationship with PETRONAS and other adverse consequences.

1.2 Using this Document

In this document, the recommendation for a course of action is made with varying degrees of emphasis. As a rule:

- "**shall**" indicates a course of action which is required or mandatory for legal entities/ OPUs. The English language equivalent or interchangeable term of "shall" is "must";
- "**should**" indicates a preferred course of action; and
- "**may**" indicates a possible course of action.

1.3 Document Owner and Custodianship

The document owner is Legal Compliance Department under the custodian of Subject Matter Expert Data Privacy.

1.4 Reference

Reference is made to the following frameworks, standards, or publications. Unless specifically designated by date, the latest edition of each publication shall be used or referred to, together with any supplementary/revision thereto:

PETRONAS Data Privacy Governance Documents:

1.4.1 PETRONAS Corporate Privacy Policy;

1.4.2 PETRONAS Critical Legal Areas Breach Reporting Manual; and

1.4.3 PETRONAS Data Protection Impact Assessment Guidelines.

Also see paragraph 1.0.2 above.

1.5 Terms and Definitions

1.5.1 General Terms and Definitions

The following terms and definitions are consistent as defined in these Guidelines:

Term	General Definition
HCUs	PETRONAS' holding company units
"PETRONAS"	Petroliam Nasional Berhad
"PETRONAS Group"	Refers to PETRONAS and OPUs
Operating Units ("OPUs")	Refers to legal entities incorporated or registered under the Companies Act or equivalent in each relevant jurisdiction where the PETRONAS Group operates, including wholly owned subsidiaries, partly owned subsidiaries and associates

1.5.2 Specific Terms and Definitions

Terminologies below are specific for these Guidelines:

Term	General Definition
"Personal Data"	Any information that can identify a natural person (i.e., an individual, not a legal entity) directly or indirectly.
"Data Controller"	A Data Controller (or also called Data User) in certain jurisdictions is the party that determines the purpose and means of processing Personal Data.
"Sensitive Personal Data" or "Special Categories of Personal Data"	Personal Data revealing racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, data concerning health or sex life or sexual orientation, genetic data and biometric data for the purpose of uniquely identifying a natural person, or any other categories of personal data as identified under applicable local personal data protection law. Categories of sensitive personal data may differ by jurisdiction.
"Data Processor"	A natural or legal person, public authority, agency or other body that processes personal data on behalf of the Data Controller.
"Joint Controller"	Where two or more controllers jointly determine the purposes and means of processing.
"Data Subjects"	An identified or identifiable person whose Personal Data is being processed. An identifiable person is a person who can be identified, directly or indirectly, by reference to an identifier, such as name, national identification number, location data, online identifier, or any other factors that are specific to physical, psychological, mental, economic, cultural or social identity.

"Processing"	Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automatic means, such as collection, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction (e.g., marking data for limited uses only), erasure or destruction.
"Data Breach"	Any actual or reasonably suspected breach of security leading to accidental, unlawful or unauthorised processing, destruction, alteration, disclosure, loss, acquisition or access to Personal Data.
"Personal Data Relating to Criminal Convictions or Offences"	Very highly sensitive Personal Data which may generally only be processed under the control of an official authority or where the processing is authorised by law.
"Consent"	Consent means that the Data Subject has given an indication that he/she agrees to the processing of his/her Personal Data as described in the relevant privacy statement. In some jurisdictions, this indication cannot be implied by conduct and must be a freely given, specific, informed and unambiguous indication of the Data Subject's wishes.

1.6 Abbreviations

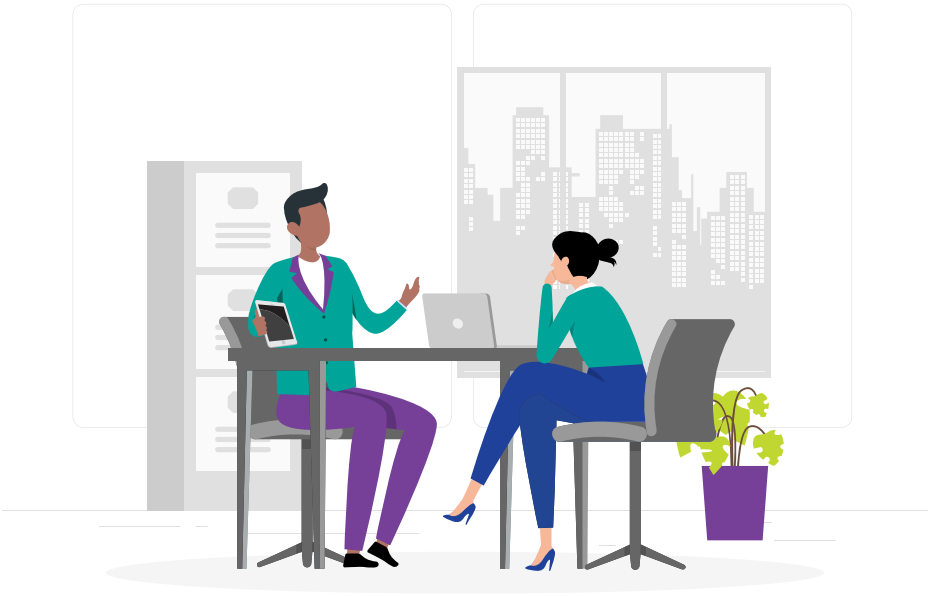
Abbreviation	Description
"COBE"	PETRONAS Code of Conduct and Business Ethics
"DPO"	Data Protection Officer
"GDPR"	General Data Protection Regulation (EU) (2016/679)
"GHRM"	Group Human Resource Management
"LCD"	Legal Compliance Department, Group Legal
"LGPD"	Lei Geral de Proteção de Dados Pessoais or Brazil's General Data Protection Law
"PDPA"	Personal Data Protection Act 2010 (in Malaysia)

Section 2: PETRONAS Corporate Privacy Policy

1.0 PETRONAS Corporate Privacy Policy states that PETRONAS is committed to complying with applicable privacy and personal data protection laws and to ensuring that the collection, use and storage of personal data relating to its employees, contractors and directors, and the third parties with whom PETRONAS works is consistent with its high standard. The core principles require that PETRONAS, in its collection, use, processing and storage of Personal Data, takes the following steps where required to do so by applicable laws:

1.0.1 to obtain adequate consent from individuals ("**Consent Principle**");

1.0.2 to provide individuals with the required notices and information, and verify that their personal data has been obtained lawfully and is relevant for the stated purposes ("**Notice Principle**");



1.0.3 to keep accurate, complete and up-to-date the personal data that has been collected ("**Accuracy Principle**");

1.0.4 to retain the personal data that has been collected only for the period necessary to fulfil the relevant purposes, unless otherwise permitted or required by applicable law ("**Retention Principle**");

1.0.5 to inform individuals concerned about the disclosure of their personal data to third party recipients ("**Disclosure Principle**");

1.0.6 to keep personal data secure by protecting it with adequate and appropriate security safeguards ("**Security Principle**"); and

1.0.7 to provide individuals with the ability to exercise their rights under applicable law, such as rights to access, rectify and/or request the erasure of their personal data, where applicable ("**Access and Correction Principle**").

1.1 As a Data Controller, PETRONAS is accountable for the lawful processing of Personal Data and must be able to demonstrate compliance with applicable data protection legislations.

1.2 Failure to comply with applicable data protection legislations may result in fines and/or imprisonment of PETRONAS' directors and officers. For example, the GDPR provides for administrative penalties of up to €20 million or up to 4% of its entire global turnover of the preceding financial year, whichever is higher. Since the coming into force of the GDPR in 2018, other countries have provided for similarly severe penalties.

1.3 Understanding the concepts and rules of personal data protection and privacy and their applicability to the ordinary course of business operations will assist in reducing the risk of infringing any applicable personal data protection and privacy law. As such, it is necessary to become familiar with these Guidelines to ensure compliance with the relevant data protection legislations.

Section 3: Key Concepts of Personal Data

1.0 What is Personal Data?

1.1 Personal Data means any information that can identify a natural person (i.e., an individual, not a legal entity) directly or indirectly.

1.2 There is another category of Personal Data, which is Special Categories of Personal Data or Sensitive Personal Data, the collection and processing of which are subject to specific rules and a higher degree of care.

1.3 Examples of what may or may not constitute Personal Data are as follows:

Personal Data	• Name and/or surname • Home address • Identification card number • Individual's email address • Employee identification number • Location data (e.g., the location data function on a mobile phone) • Internet protocol ("IP") address • Cookie identifiers • Information about activities of individuals (e.g., purchase history, browsing behaviour)
Special Categories of Personal Data or Sensitive Personal Data	• Race or ethnic origin • Religious and philosophical beliefs • Political opinion • Trade union membership • Data concerning health or sex life or sexual orientation • Genetic data • Biometric data
Not Personal Data	• Company registration number • Organisation email address (e.g., info@company.com; contactus@company.com) • Pure factual data relating to things and not to persons (e.g., costs of a product, name of a vessel, technical data) • Pure statistical data (e.g., market data from research companies) • Anonymised data

1.4 Different pieces of information which when compiled can lead to the identification of a particular person is Personal Data. For example, whilst individual information such as physical attributes, gender, race and department in PETRONAS will not identify a person, this information collectively could identify the specific employee and will be considered Personal Data.

Example of collection of anonymised data leading to identification:

Staff A was tasked to collect non-identifiable anonymised data on a number of male employees aged 50 and above who have underlying medical problems such as diabetes in Germany. However, if there is only a single individual age 50 and above in Germany, age and gender data will allow identification of the individual. As such, collection of the health data of the employee must be done in compliance with personal data protection laws in Germany.

1.5 Personal Data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person is still Personal Data and falls within the scope of personal data protection laws.

1.6 Personal Data that has been rendered anonymous in such a way that the individual is not or no longer identifiable is no longer considered Personal Data. For Personal Data to be truly anonymised, the anonymisation must be irreversible. See Section 5 paragraph 5.0 for further information on anonymised and pseudonymised Personal Data.

2.0 Concept and Responsibility: Data Controller, Data Processor and Joint Controller

2.1 When handling Personal Data, it is important to understand the concept and responsibility of Data Controller (also known as Data User), Data Processor and Joint Controller due to the different legal obligations imposed upon these parties to ensure the Personal Data is lawfully processed and adequately protected.

2.2 The following are general definitions and examples of the terms Data Controller, Data Processor and Joint Controller:

2.2.1 Data Controller:

A Data Controller (or also called Data User) in certain jurisdictions is the party that determines the purposes and means of processing Personal Data. Depending on jurisdiction, the Data Controller can be a natural or legal person, public authority, agency or other body which, individually or jointly with others, determines the purposes and means of the processing of Personal Data.

Example:

PETRONAS is the Data Controller for its employees' Personal Data as it determines the purpose of processing the employees' Personal Data.

2.2.2 Data Processor:

A Data Processor processes Personal Data at the instruction of the Data Controller. A Data Processor should not process Personal Data other than for the purposes set out by the Data Controller.

Example:

When PETRONAS appoints a third-party service provider to manage or support the operations of its finance and/or human resources functions for its employees (e.g., payroll, insurance etc.), the third-party service provider would be a Data Processor if it is acting based on instructions from PETRONAS.

2.2.3 Joint Controller:

When two or more parties determine the purpose and means of processing, both parties may be considered as Joint Controllers.

Examples:

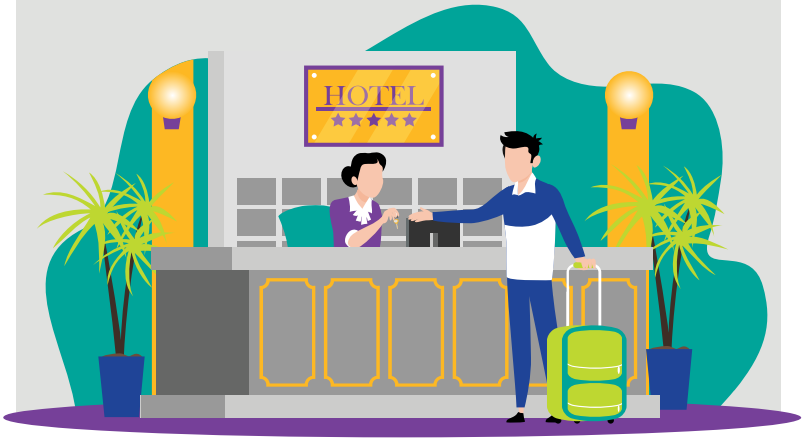
Scenario 1: No Joint Controllership

A travel agency sends the Personal Data of its customers to the airline and a chain of hotels, with a view to making reservations for a travel package.

The airline and the hotel confirm the availability of the seats and rooms requested.

The travel agency issues the travel documents and vouchers for its customers.

In this scenario, the airline, hotel and travel agency each processes the Personal Data to carry out their own activities using their own means. Each of the three different data controllers are processing Personal Data for their own and separate purposes and there is no joint controllership.



Scenario 2: Joint Controllership

The travel agency, the hotel chain and the airline jointly set up an internet-based common platform for the common purpose of providing package travel deals. They agree on the essential means to be used, such as which Personal Data will be stored, how reservations will be allocated and confirmed, and who can have access to the information stored and can share the Personal Data of their customers in order to carry out joint marketing actions.

In the above scenario, the travel agency, the airline and the hotel chain all jointly determine why and how the Personal Data of their respective customers are processed and will therefore be joint controllers with regard to the processing operations relating to the common internet-based booking platform and the joint marketing actions.

However, each of them would still retain sole control with regard to other processing activities outside the internet-based common platform.

2.3 The key responsibilities of Data Controllers, Data Processors and Joint Controllers are as set out below:

2.3.1 The key responsibilities of a Data Controller include, among others, to ensure that:

(i) Personal Data is collected lawfully and only used for the purposes for which it is provided;

(ii) Data processing is notified to individuals and individuals can exercise certain rights over their Personal Data;

(iii) Personal Data is not retained for longer than necessary;

(iv) Technical and organisational security measures are adopted to protect Personal Data against loss, damage or destruction; and

(v) Personal Data is kept accurate and updated.

2.3.2 Responsibility of Data Processor

A party acting as a Data Processor must ensure the following:

(i) That it only processes Personal Data on instruction from the Data Controller (unless otherwise required by law);

(ii) That it takes appropriate measures to maintain the security of the Personal Data and to prevent the Personal Data from being lost, altered, damaged or accessed by people who are not authorised to have access to it; and

(iii) That it provides adequate guarantees to the Data Controller to ensure the implementation of security and confidentiality as the Data Controller remains legally responsible for that Personal Data even though it may no longer have direct control over it.

These guarantees should be included in the contract between the Data Processor and the Data Controller, which should include, but is not limited to, embedment of Compliance Clauses in the contract provided herein in Appendix II – Personal Data Protection Compliance Clauses.

2.3.3 Responsibility of Joint Controller:

(i) Each of the Joint Controllers have the same responsibility as a Data Controller under paragraph 2.3.1 above.

(ii) Further, the Joint Controllers shall in a transparent manner, expressly determine their respective responsibilities in relation to the processing of Personal Data.

Section 4: Collection of Personal Data

1.0 Lawful Basis of Processing

1.1 A Data Controller may only validly process Personal Data if there is a lawful basis for such processing.

1.2 There are various lawful bases for processing as described under local privacy laws. It is up to Data Controller to identify what is the valid lawful basis which can be relied on in processing Personal Data. There may be more than one lawful basis for processing of the same Personal Data.

1.3 Different jurisdictions may specify slightly different lawful bases. For example, legitimate interest is not permitted as a lawful basis under Malaysia and China Personal Data Protection Laws. On the other hand, Singapore PDPA and LGPD has additional lawful bases for processing not prescribed under privacy laws in other countries.

1.4 The relevant legal basis for processing must typically be described in the related privacy notice for collection of that Personal Data.

1.5 The following are key lawful bases for processing:

i. Consent from the Data Subject;

ii. Contractual necessity;

iii. Need to comply with legal obligations;

iv. Need to protect the Data Subject's vital interests;

v. Need for the performance of tasks carried out in the public interest; or

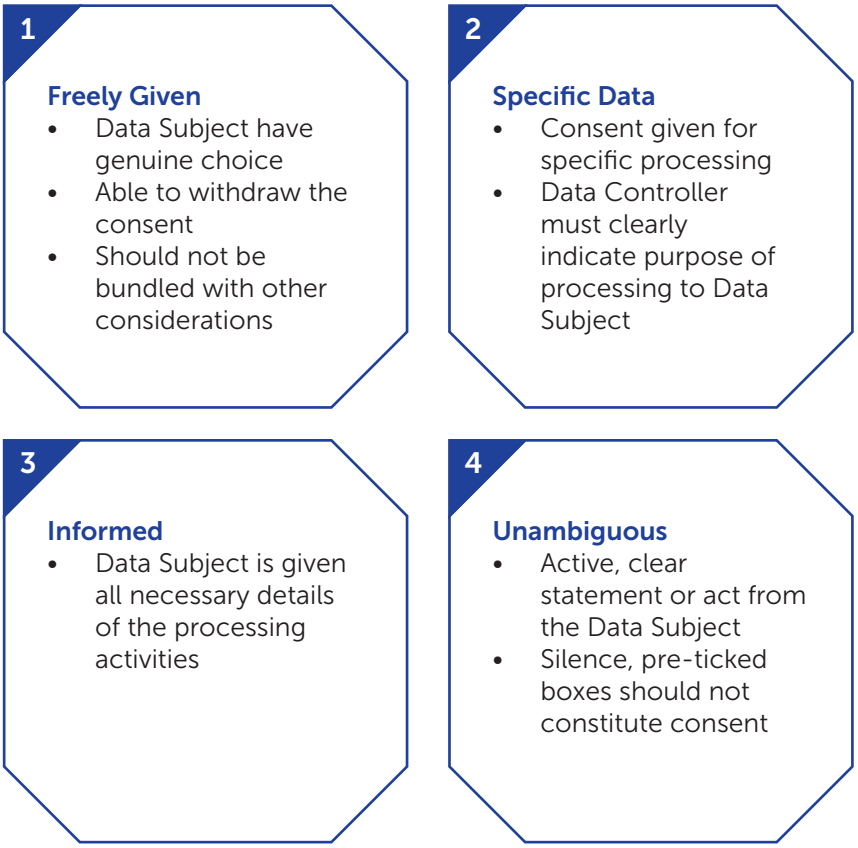
vi. Legitimate interest of Data Controller in processing the Personal Data.

1.6 Additionally, when sensitive data or Personal Data relating to criminal convictions or offences is involved, some jurisdictions may impose additional requirements.

2.0 Consent

2.1 Where consent is relied on as the legal basis for processing, a Data Controller must obtain consent from individuals whose Personal Data is collected prior to the processing of that Personal Data.

2.1.1 Such consent must generally be freely given, specific, informed and unambiguous. The following table provides clarification on the specific elements required for a valid consent:



2.1.2 The following information should be provided to enable informed consent of the Data Subject:

(i) The Data Controller's identity;

(ii) The kind of Personal Data that will be processed;

(iii) The purpose of each of the processing operations for which consent is sought;

(iv) The existence of the right to withdraw consent;

(v) Information about the use of automated decision making if applicable; and

(vi) Transfer of Personal Data and any risk associated with the data transfer and safeguards that are put in place.

2.1.3 Examples of freely given, specific, informed and unambiguous consent:

(i) **Freely Given:**

A mobile app for photo editing asks its users to have their GPS localisation activated for the use of its services. The app also tells its users it will use the collected data for behavioural advertising purposes. Neither geolocalisation or online behavioural advertising are necessary for the provision of the photo editing service and go beyond the delivery of the core service provided. Since users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given.

A bank asks customers for consent to allow third parties to use their payment details for direct marketing purposes. This processing activity is not necessary for the performance of the contract with the customer and the delivery of ordinary bank account services. If the customer's refusal to consent to this processing purpose would lead to the denial of banking services, closure of the bank account or, depending on the case, an increase of the fee, consent cannot be considered to be freely given.

(ii) **Specific**

A cable TV network collects subscribers' Personal Data, based on their consent, to present them with personalised suggestions for new products they might be interested in based on their viewing habits. After a while, the TV network decides it would like to enable third parties to send or display targeted advertising based on the subscribers' viewing habits. Given that subscribers have not specifically provided consent for their Personal Data to be shared for third parties' targeted advertising, new consent is needed.

(iii) **Informed**

A company processes Personal Data on the basis of consent. The company uses a layered privacy notice that includes a consent request. The company discloses all basic details of the data controller, the data processing activities envisaged and the purposes of the processing, thus allowing the entity to have informed consent.

(iv) **Unambiguous**

Swiping a bar on a screen or waving in front of a smart camera may be positive options to indicate agreement, as long as clear information is provided, and it is clear that the motion in question signifies agreement to a specific request (e.g., "if you swipe this bar to the left, you agree to the use of information X for purpose Y. Repeat the motion to confirm."). The Data Controller must be able to demonstrate that consent was obtained this way and Data Subjects must be able to withdraw consent as easily as it was given.

2.2.3 The consent obtained must be recorded and retained by Data Controller throughout the processing period. This is important because regulators may require the company to provide evidence that it has obtained the required consent of Data Subject for the processing undertaken.

2.2 Explicit Consent

2.2.1 Depending on the jurisdiction, the processing of the following categories of Personal Data requires explicit consent from the Data Subject:

(i) Special Categories of Personal Data or Sensitive Personal Data

(ii) Automated decision making with legal effects or that significantly affects the Data Subject

(iii) Transfer of Personal Data to other countries.

2.2.2 The term explicit refers to the way consent is expressed by the Data Subject. It means that the Data Subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the Data Controller could make sure the written statement has been signed by the Data Subject in order to remove all possible doubt and potential lack of evidence in the future.

2.2.3 In a digital or online context, a Data Subject may be able to issue the required statement by filling in an electronic form, sending an email, uploading a scanned document or using an electronic or digital signature.

2.2.4 Explicit consent may also be obtained through a telephone conversation, provided that the information about the choice is fair, intelligible and clear, and it asks for a specific confirmation from the Data Subject (e.g., pressing a button or providing oral confirmation). Any such consent should be recorded.

2.2.5 For example, when you are collecting the vaccination status of an employee, you must ensure explicit consent is obtained as vaccination status is identified as Sensitive Personal Data of a person.

2.2.6 Similar to paragraph 2.1.4, the explicit consent must be recorded and retained by Data Controller throughout the processing period.

2.2.7 In light of the above, please note the following:

(i) Passive behaviour may not be acceptable under the strictest Personal Data protection regimes (e.g., where the Data Subject continues exploring a website despite a notice or banner which refers to the relevant privacy policy).

(ii) Affirmative action is required and that includes, for instance, an oral statement given to a telemarketer, a handwritten signature or the checking of a box or clicking on a button/link to demonstrate consent.

2.3 Invalid Consent

2.3.1 In certain jurisdictions, such as under the GDPR, the imbalance of power between the Data Controller and Data Subject can lead to consent being invalid and not freely given.

2.3.2 In that jurisdiction, consent is not regarded as freely given if the Data Subject has no genuine free choice or is unable to refuse or withdraw consent without detriment. This may be an issue where the Data Controller is a public authority or an employer.

2.3.3 For example, under the GDPR, an imbalance of power is likely to exist in an employment context between employers and employees. Employees' consent may be deemed to be invalid as there may be adverse consequences to the employees' employment if they do not provide consent.

2.3.4 In light of the above, it is generally recommended to rely on an alternative lawful basis for processing Personal Data where there is an imbalance of power.

2.4 Minors

2.4.1 Most personal data protection laws provide specific protection over Personal Data of children. For example, under the GDPR, consent obtained from children under the age of 16 years on the basis of consent will be lawful only if the consent is given or authorised by the holder of the parental responsibility over the child. Under Malaysian law, minors are children under the age of 18.

2.4.2 Therefore, it is necessary to check the applicable local personal data protection laws before collecting and processing Personal Data from children.

3.0 Legitimate Interests

3.1 Where Consent cannot be relied on as lawful basis of processing, in certain jurisdictions, for example, under the GDPR, a Data Controller can consider its legitimate interests as the lawful basis for processing Personal Data.

3.2 Data Controllers may process Personal Data pursuant to their legitimate interests, provided that such interests are not overridden by the rights and freedom of Data Subject.

3.3 In balancing the interests of the Data Controller and the Data Subject, the Data Controller must satisfy the legitimate interests test as follows:

(i) **Purpose test**

(a) Considering whether the intended processing of the Data Subject's Personal Data is for a legitimate purpose.

(ii) **Necessity test**

(a) Demonstrating that the intended processing of the Data Subject's Personal Data is necessary to achieve the purpose.

(b) The Personal Data must be proportionate and not intrusive.

(iii) **Balancing test**

(a) Balancing the Data Controller's legitimate interests against the Data Subject's interests, rights and freedoms.

(b) The purpose of processing shall not override the rights and freedom of Data Subject.

3.4 Examples of processing on the basis of legitimate interests:

(i) **For prevention of fraud**

Where the processing of Personal Data is strictly necessary for the purpose of preventing fraud.

(ii) **Transmission within the company group for administrative purposes**

Where the Data Controller is part of an undertaking or affiliated institutions and may have a legitimate interest in transmitting Personal Data within the company group (subject to the general principles of transferring Personal Data to a third country).

(iii) **Ensuring network security**

Processing Personal Data to the extent strictly necessary and proportionate for ensuring network and information security (subject to the general principles of transferring Personal Data to a third country).

(iv) **Reporting possible criminal acts**

Indications of possible criminal acts or threats to public security and transmitting the relevant personal data to a competent authority by the Data Controller. Further processing by the Data Controller is prohibited if the processing is not compatible with legal, professional and other binding obligations of secrecy.

4.0 Other Lawful Bases

Apart from consent and, in certain jurisdictions, legitimate interests, there are other lawful bases that can be relied on in processing Personal Data. They include:

4.1 Contractual Necessity

For the conclusion or performance of a contract with individuals where the Data Controller and the Data Subject are the parties to the contract.

For example, when you purchase products online, the company will need your address and phone number to be able to deliver the products to you.

4.2 Legal Obligations

Processing is required where a Data Controller needs to comply with legal obligations, such as when an employer is required to disclose employee salary information to comply with applicable taxation laws or when a court provides directions to process Personal Data for a particular purpose.

4.3 Vital Interests

The processing is essential for the life of the Data Subject.

For example, processing the Data Subject's medical records in an emergency situation as a means to protect the Data Subject's life.

4.4 Public Interests

Processing is required for the performance of tasks carried out in the public interest.

This legal basis applies to public authorities with the power provided by law to process personal data for their public tasks.

5.0 Privacy Notice

5.1 A privacy notice, or also known as a privacy statement, explains how the Personal Data of Data Subjects will be collected and used. This is an easy way of communicating with Data Subjects what their information is being used for and how it will be processed. Data Subjects should be able to read the privacy statement before deciding whether to provide the information.

5.2 It is therefore recommended to include a reference or link to PETRONAS' privacy notice at the collection point/when collecting Personal Data.

A privacy notice must generally include at the minimum the following information:

(i) To specifically state the details of the Personal Data involved, including:

(a) types of Personal Data including any Sensitive Personal Data;

(b) mentioning if the Personal Data of minors are being processed;

(ii) The sources where the Personal Data is collected from;

(iii) The purpose of processing that Personal Data, including if there is any legal requirement for collection of that Personal Data and the lawful basis for processing;

(iv) How long and how it will be stored:

(a) state the retention period and when the Personal Data will be disposed of;

(b) state the practical measures taken to ensure the Personal Data will be securely stored;

(v) Third parties to whom the Personal Data will be disclosed:

(a) identify the categories of third parties to whom the Personal Data are disclosed to and the purpose of disclosure;

(b) stating the security measures in place to ensure the disclosure implemented is safe and secure;

(vi) Data Subject rights (depending on jurisdiction):

(a) Personal Data submission choice – whether this is compulsory or optional. If it is compulsory, specify the consequences of not submitting it;

(b) how the Data Subject may access, correct or update the Personal Data submitted;

(c) how the Data Subject may limit the processing of the Personal Data submitted;

(d) how the Data Subject may withdraw consent to the processing of Personal Data; and

(vii) Who to contact with queries or complaints: provide relevant contact information.

5.3 In addition to the above, there may be specific country legal requirements of information to be disclosed in a privacy notice. For example:

(i) a legal requirement for the privacy notice to also be in the local language;

(ii) specific guidelines on the format of the privacy notice e.g., layout, headers and font to ensure easy readability of the privacy notice;

(iii) location where the privacy notice will be placed, i.e., if physical notice, at a strategic location; and

(iv) stating effective data and review dates in the privacy notice to inform Data Subjects on any changes made to the privacy notice.

Therefore, privacy notices need to be prepared in accordance with the requirements of personal data and privacy laws of the country.

5.4 Most regulators emphasise the need for a privacy notice to be in simple language and easy to read to ensure that the relevant Data Subjects, particularly minors, understand the privacy notice.

5.5 See **Appendix III- Templates of PETRONAS Privacy Notices** for reference. Please consult LCD if you are reviewing or developing a privacy notice in your day-to-day operations.

Section 5: Management and Control of Personal Data: Accountability

1.0 General Accountability Obligation

1.1 A Data Controller is accountable for the lawful processing of Personal Data and must be able to demonstrate compliance with applicable personal data protection and privacy laws.

1.2 Generally, the accountability obligation will apply to all activities which involve the processing of Personal Data.

1.3 Particular attention should be given to the following categories of Personal Data:

(i) **Employee Personal Data:**

Processing these types of Personal Data is necessary for PETRONAS Group to carry out its obligations and exercise its rights to its employees.

Examples of processing for employment purposes include for the purposes of hiring, payroll, career progression, notifications to tax administration, payment of social contributions, management of company vehicles, payment cards, elections of employee representatives, IT network services and corporate e-mails.

Further details on processing of employees' Personal Data are provided in Section 10 of these Guidelines.

(ii) **Marketing on Customer's Personal Data:**

PETRONAS may process Personal Data for marketing purposes. This includes providing promotional, web-based or telemarketing material to customers and potential customers.

Further details on marketing are provided in Section 9 of these Guidelines.

1.4 The rest of this Section 5 sets out key measures for how to demonstrate compliance with a general obligation to be accountable for the processing of Personal Data.

2.0 Data Protection by Design and Default

2.1 When designing new processes for handling Personal Data, or in commissioning new data handling systems or processes, all reasonable steps must be taken to ensure that appropriate privacy safeguards are embedded, and that, by default, Personal Data is processed only to the extent necessary to achieve legitimate business purposes.

Don't forget!

*Remember to think about **data protection considerations when designing any new data handling process or implementing any new data handling system.***

For example, is the collection of personal data limited to what is directly necessary for the specified purpose? Would the personal data still serve its purpose if it was anonymised to prevent inadvertent disclosure and security breaches? Do not ignore personal data considerations as they are easier to implement at the outset when designing a process or system, rather than after the process or system is set up.

2.2 Personal Data protection and privacy requirements must be placed at the forefront of PETRONAS' operations by design and considered when putting in place the means by which PETRONAS processes Personal Data.

2.3 Any database of Personal Data should incorporate data fields that are designed to enable the quick identification of:

(i) the Personal Data collected;

(ii) the purpose(s) for which it was collected; and

(iii) whether, at any point in time, it is necessary to keep retaining the Personal Data for said purpose(s).

3.0 Data minimisation

3.1 Limit collection of Personal Data to what is adequate, relevant and necessary in relation to the purposes of processing.

3.2 Retain only the minimum Personal Data necessary for the purposes of processing. Consider the purpose for which the Personal Data is collected, and what is adequate, relevant and necessary to achieve that purpose. Make the assessment separately for each individual (or group of individuals sharing the same characteristics) whose Personal Data is collected.

3.3 For example, when processing the vaccination status of employees for the purposes of reopening the workplace, consider omitting the name of the employee and limiting the collection to the type of vaccine and date of vaccination if this is the only required information for processing.

4.0 Accuracy

4.1 Take every effort to ensure that Personal Data is accurate and up to date, including reviewing the Personal Data kept and considering whether steps need to be taken to confirm its accuracy, or, alternatively, whether it should be rectified or erased.

4.2 For example, employees can update their Personal Data for employment purposes in the system used by PETRONAS Group, such as myPassport and myCareerX.

5.0 Anonymisation/Pseudonymisation

5.1 There may be circumstances in which the processing of Personal Data can be appropriately limited so that the data:

(i) no longer allows attribution to a specific Data Subject ("anonymisation"); or

(ii) allows attribution to a specific Data Subject only by using additional separate information ("pseudonymisation").

5.2 The following table explains the important distinction between anonymisation and pseudonymisation:

Anonymisation
• The modification of Personal Data with the aim of irreversibly preventing the identification of the individual to whom it relates. • Personal Data can be considered effectively and sufficiently anonymised if it does not relate to an identified or identifiable natural person or where it has been rendered anonymous in such a manner that the Data Subject is not or no longer identifiable. • Only if the Data Subject is no longer identifiable under this standard is the information no longer Personal Data. • Knowledge about the effectiveness of various anonymisation techniques is constantly changing. It is therefore impossible to say that a particular technique will be 100% effective in protecting the identity of Data Subjects. • "Identification" in the case of anonymisation means the possibility of retrieving a person's name and/or address, but also potential identifiability by singling out, linking ability and inference. • Personal Data which has been irreversibly anonymised ceases to be "personal data", and the processing of such data does not re-quire compliance with personal data protection laws. • In principle, this means that organisations could use it for purposes beyond those for which it was originally obtained, and that it could be kept indefinitely.

Pseudonymisation
• The replacement of any identifying characteristics of Personal Data with a pseudonym, or, in other words, a value which does not allow the Data Subject to be directly identified. • Pseudonymisation only provides limited protection of the identity of Data Subjects in many cases as it still allows identification using indirect means. • Where a pseudonym is used, it is often possible to identify the Data Subject by analysing the underlying or related data. • As it is still possible to combine additional information to identify the individual with the pseudonymised data, the pseudonymised data is still Personal Data and data protection legislation is fully applicable.

Don't forget!

Only if the Data Subject is no longer identifiable under this standard is th information no longer Personal Data.

Do not treat personal data as being anonymised if they are only pseudonymised. There is a risk that anonymised data may be re-identified which can occur when an individual is identifiable from the dataset, even when combined with other information. Steps to miminise the risk of re-identification may include limiting the number of data recipients that will receive the information and limiting the number of people that have access to the information.

5.3 Always consider the possibility and appropriateness in applying anonymisation or, at least, pseudonymisation, based on the feasibility and requirements of the scenario.

6.0 Audits

According to the accountability principle, in order to demonstrate compliance with the general key requirements set out in these Guidelines and other applicable data protection and privacy law requirements, internal audits of processing activities are required to be undertaken from time to time. Full cooperation with the audit is necessary.

7.0 Special Care in Respect of Sensitive Personal Data or Personal Data Relating to Criminal Convictions or Offences

7.1 When processing Sensitive Personal Data, take extra care and ensure additional safeguards are in place. For example, obtaining Data Subjects' express consent where it is required.

7.2 Additional safeguards include controlling access of the Personal Data, ensuring the Sensitive Personal Data is kept separately so that it can be accessed on a need-to-know basis and/or deleted independently of other Personal Data. In any event, it must be possible to identify it and control what it is used for.

7.3 Personal Data relating to Criminal Convictions or Offences can only be collected based on legislative provisions that allow collection under relevant personal data protection laws (where applicable). The safeguards set out in paragraph 7.2 above are equally applicable to Personal Data relating to Criminal Convictions or Offences.

8.0 Purpose Limitation

8.1 Ensure that Personal Data is only collected for specified, explicit and legitimate purposes permitted under applicable data protection laws. Where relying on consent as the lawful basis of processing, the individuals should have consented to those purposes of processing.

8.2 Be transparent about the purposes for collecting the Personal Data and specify the intention for use of the Personal Data.

8.3 Personal Data should not be further processed for a new purpose that is very different than the initial purpose. If this happens, you should seek specific consent to use the Personal Data for the new purpose.

8.4 In some jurisdictions, there may be requirements that the purposes of processing are reasonable or proportionate.

9.0 Record of Processing Activity ("ROPA")

9.1 It is advisable to maintain a ROPA to demonstrate compliance with the personal data protection and privacy requirements. In certain jurisdictions, such as the EU, maintaining the ROPA can be a legal obligation and failure to do so will result in fines by the regulator.

9.2 The ROPA should contain at the minimum, the following information:

(i) Parties involved in the processing of the Personal Data (including controllers; processors, etc.);

(ii) Purpose of processing (i.e., the reason why you collected the Personal Data);

(iii) Categories of data subjects and Personal Data;

(iv) The category of recipient for this Personal Data; and

(v) Time limits provided for the erasure of this Personal Data.

Please refer to specific jurisdictional requirements in developing and maintaining the ROPA.

10.0 Data Protection Impact Assessment ("DPIA")

10.1 A DPIA is an important process to build and demonstrate compliance. It is an assessment undertaken on proposed operations or projects on the protection of Personal Data, the proportionality of the processing and the risks to the rights and freedom of Data Subjects, taking into account the nature, scope and context and purposes of the envisaged processing of Personal Data.

10.2 In certain jurisdictions a DPIA is mandatory when the collection and use of Personal Data is likely to result in a high risk to the rights or freedoms of individuals.

10.3 In order to determine whether the processing is likely to result in a high risk to the rights and freedom of individuals, a pre-assessment needs to be conducted as detailed in the PETRONAS Data Protection Impact Assessment Guideline. An example of a processing which is likely to result in high risk to the rights and freedom of individuals include:

(i) Systematic and extensive processing activities, including profiling and where decisions have significant effects on an individual. For example, where there is a need to install tools to monitor employee internet activity for security purposes.

(ii) Large scale monitoring of public areas. For example, installation of CCTV in public areas.

10.4 When you are processing personal data in a system, please refer to Group Digital for the conduct of DPIA which form part of the PETRONAS Cybersecurity Control Procedures for SME - Cyber Security Regulatory Compliance – Data Protection Impact Assessment ("DPIA").

11.0 Appointment of a Data Protection Officer ("DPO")

11.1 Certain jurisdictions require a mandatory appointment of a DPO to oversee organisational privacy programmes.

11.2 The appointment, obligations and duties of the DPO must comply with the legal and regulatory requirements of such jurisdiction or country.

11.3 Even where there is no mandatory obligation, a DPO may be appointed in order to strengthen monitoring and ensure compliance with personal data protection and privacy laws.

11.4 DPOs have various tasks, including among others:

(i) Advising the company for which they are appointed and its employees on their obligations pursuant to data protection and privacy laws;

(ii) Monitoring compliance with these laws and with PETRONAS policies on the protection of Personal Data;

(iii) Cooperating with data protection authorities; and

(iv) Being the point of contact for individuals exercising rights under applicable data privacy legislation.

12.0 Training and Awareness

12.1 Employee training is a crucial part of the culture of accountability towards personal data protection in personal data protection laws. This includes creating awareness of data protection issues amongst all employees across all roles, functions, and hierarchy in the company.

12.2 Raising awareness enables employees to understand data protection legal requirements and raise privacy awareness and standards.

12.3 Employees whose roles specifically include handling personal data (e.g., marketing and sales) or implementing security (e.g., IT) are required to be diligent in adhering to applicable personal data protection laws, policies and procedures and hence require more focused and mandatory data protection training.

12.4 See **Appendix IV - Checklist to Develop and Monitor Personal Data Protection Training Programmes.** The checklist can be used to:

(i) Check existing practices to expected regulatory standards or expectations for personal data protection;

(ii) Highlight considerations for improvements in existing practices in specific areas; and

(iii) Record, track and report on progress in order to demonstrate compliance.

12.5 Please note that personal data protection regulators in certain jurisdictions may have specific expectations with regard to the conduct of personal data awareness and training programmes. For example, the Data Breach Notification Form issued by the UK Information Commissioner's Office includes the following questions with regards to training:

(i) Has the staff member involved in the breach received data protection training in the last two years; and

(ii) Please describe the data protection training you provide including the outline of training content and frequency.

Section 6: Transferring Personal Data to Different Countries

1.0 Personal Data Transfer Obligations

1.1 In the course of business, it is possible that there is a need to send Personal Data about data subjects (for example, employees or customers) to a third party or another PETRONAS Group or a third-party service provider located in another jurisdiction. When doing this, be mindful that restrictions to such transfers exist under various personal data protection and privacy laws. The rules are different depending on the applicable data protection and privacy legislation and on the location of the third party where the Personal Data will be transferred.

1.2 Identify the jurisdiction involved in the transfer, including its origins and where the Personal Data is intended to be hosted and shared. This is to ensure that there are sufficient controls in place to ensure compliance with the privacy requirements in the originating country while at the same time complying with the local requirements of the jurisdiction or country where the Personal Data will be transferred to.

1.3 Reference can be made to any applicable data transfer agreement (e.g., PETRONAS Group Data Transfer Agreement for the transfer of personal data within PETRONAS Group or other third-party data transfer agreement).

1.4 In addition to having agreements in place prior to the transfer, please ensure other controls have been implemented, such as notifying the Data Subject of the transfer, obtaining consent (if applicable) from the Data Subject, embedding technical controls (e.g., password protected, encryption of document etc.), properly recording transfer activities, undertaking a Transfer Impact Assessment ("TIA") and DPIA where required, and other relevant controls that are necessary under local laws.

1.5 Please note that some of these assessments such as TIA or DPIA requires ample time for completion. Therefore, do take into consideration and ensure that there is sufficient time and resources necessary for projects that require the transfer of Personal Data to different countries.

Don't forget!

When transferring Personal Data between countries, you must conduct an analysis of the data flows involved to ensure any transfers of personal data out of a jurisdiction is compliant with the data transfer requirements of that jurisdiction.

If data is transferred between more than two countries, you may need to do an analysis of each country's local laws to ensure that any transfers are compliant with their data protection requirements. Do not transfer personal data overseas without complying with these requirements which may be complex and require legal analysis.

Section 7: Data Subject Rights

1.0 General Rights of Data Subject

1.1 Data Subjects generally have rights over the Personal Data held about them. This allows them to retain control over their information and require processing to cease if they choose so. Nevertheless, in certain cases, processing may be allowed even if the relevant Data Subject does not agree, such as, for instance, in the context of litigation or when the employer is required to comply with legal obligations.

1.2 In general, Data Subject rights include (depending on jurisdiction):

(i) The right to be informed about the collection and use of their Personal Data and request confirmation as to whether or not their Personal Data is being processed.

(ii) The right to ask about the type of processing of their personal data, the purpose of the processing, the source of personal data held about them (i.e., where the Personal Data was obtained from) and the recipient or categories of recipients to whom the Personal Data will be disclosed.

(iii) The right to ask for how long their Personal Data will be stored.

(iv) The right to access and receive copies of Personal Data held.

(v) The right to request that their Personal Data be updated and/or to correct information about them when that information is obsolete or incorrect and the right to have their Personal Data deleted.

(vi) The right to ask that the way their Personal Data is processed is restricted or suppressed.

(vii) The right to object to the processing of their Personal Data.

(viii) The right to ask to be provided with a copy of their Personal Data in a form that enables them to transfer it to a different provider or ask us to transfer it for them.

(ix) The right to be informed of any automated decision-making, including profiling used in connection with their Personal Data.

(x) The right to lodge a complaint with the relevant data protection regulatory authority as further stated below.

1.3 It is possible to refuse to act on a request of a Data Subject (or charge a reasonable fee, subject to local privacy laws) if it can be demonstrated that such request is manifestly unfounded or excessive (in particular because of its repetitive character). In any event, in case of a suspicion that a request is frivolous or vexatious, instead of not responding, such circumstances and related evidence should be sent to LCD in determining the proper response to such request.

2.0 Manner and Timing of Responding to Data Subject Access Request

2.1 Data Subjects' enquiries may come in directly by fax, e-mail or post or by any other means, including those listed in PETRONAS' privacy notice.

2.2 Practical steps that must be taken when you receive a request for information include:

(i) Determine whether there is a legal basis for the request, and always acknowledge the request as soon as possible.

(ii) Assessment should be made to determine whether the request is legitimate, and it is not manifestly unfounded or excessive and how the request should be properly responded to.

(iii) All requests should be dealt with promptly as some jurisdictions impose strict deadlines for response and we may be fined if we do not adhere to such deadlines. For example, the Malaysia PDPA requires the response to Data Subject within 21 days of the date of the access request whereas under the GDPR, it is one month from the request which can be extended. Therefore, it is necessary to check local requirements.

(iv) Only provide personal information to the actual Data Subject. As such, ensure the identity of the Data Subject is properly verified.

(v) Only provide the information that is requested by the Data Subject if it is not vexatious or excessive as specified in paragraph 1.3 above.

2.3 If a request for restriction is received, establish whether it is a valid request. Please note that under the Personal Data protection and privacy laws of certain jurisdictions, when a Data Subject has requested that processing be restricted, in the absence of the Data Subject's consent, personal data can only be processed for limited purposes such as in relation to a legal claim or to comply with legal obligations.

2.4 Please refer to **Appendix V - Guide in Handling Data Subject Access Request** for detailed high-level guidance to responding to a request from a Data Subject.

3.0 Complaint Handling

3.1 Data Subjects have a right to lodge a complaint with the relevant data protection regulatory authority. The authority will then have the right to investigate the matter.

3.2 Complaints/requests received from Data Subjects/any data protection regulatory authority should be treated seriously and dealt with efficiently and promptly. If you receive such a complaint, you should immediately bring it to the attention of LCD and the DPO (if applicable) to resolve the complaint.

3.3 The complaints/requests and responses provided should be documented properly for record purposes, together with any relevant documents.

Section 8: Personal Data Breaches

1.0 Security Incidents and Personal Data Breaches

1.1 Personal Data breaches may pose significant risks to PETRONAS.

1.2 Personal Data breaches may arise from the following:

(i) **Confidentiality Breach**

Where there is an unauthorised or accidental disclosure of, or access to, Personal Data.

(ii) **Integrity Breach**

Where there is an unauthorised or accidental alteration of Personal Data.

(iii) **Availability Breach**

Where there is an accidental or unauthorised loss of access to or destruction of Personal Data.

1.3 The common causes for a Personal Data breach may be due to cyber-attacks, improper handling of Personal Data, actions of rogue employees and lack of training.

1.4 For example, if an employee's laptop is stolen and it contains an unencrypted customer database which consists of customers' name, IC, phone number, address and date of birth, this may constitute a Personal Data breach as the leaked information may pose a high risk to the affected individuals, such as persons impersonating the affected individual.

1.5 Some jurisdictions require organisations to notify the data breach to the regulator within a specific and very short deadline. For example, in the EU, organisations are expected to notify the regulator within 72 hours after having become aware of the breach, whereas in Brazil the deadline is 48 hours.

1.6 Some jurisidictions will also require organisations to notify individuals affected by the breach where the breach is likely to result in a high risk to the rights of the individual.

1.7 The following information needs to be collated to ensure the breach is handled and mitigated in a timely manner:

(i) Description of the breach;

(ii) Chronology of the event;

(iii) Data Subject involved;

(iv) Types of Personal Data involved;

(v) When it was identified;

(vi) Affected parties;

(vii) Likely consequences of the breach;

(viii) Measures taken/proposed to be taken to mitigate any adverse effects; and

(ix) Other information which may be relevant.

1.8 In the event of occurrence or potential occurrence of a Personal Data breach incident, please refer to PETRONAS Data Breach Notification Protocol in order to respond to the incident/breach. There may be serious repercussions and consequences for PETRONAS to regulators and/or individuals, as a result of any such breach of Personal Data.

Don't forget!

Immediately escalate any actual or suspected breach internally. There may be substantial financial penalties in addition to significant reputational impact if there is a delay in responding to such any such cyber incidents.

In some jurisdictions, there are very short data breach notification deadlines to inform any relevant regulators as well as affected individuals. Failure to notify the relevant regulators or impacted individual on time may result in severe repercussions for PETRONAS.

Section 9: Communications with Customers and Stakeholders

1.0 General Communication

1.1 Communication with stakeholders or sending direct marketing to customers often triggers not only data protection requirements, but also consumer protection regulations that vary from country to country. In some jurisdictions, separate rules may apply for telemarketing or for sending SMSes or emails.

1.2 Failure to understand the application of data protection regulations when sending communications to stakeholders or direct marketing to customers may be detrimental to PETRONAS. For instance, if appropriate marketing consents are not collected, marketing communications sent to individuals who do not want to receive them may attract compliance risks, including, but not limited to, significant fines, losing valuable client goodwill and reputational damage to the company.

1.3 When processing an individual's Personal Data for these purposes, consider the following:

(i) Ensure that there is a lawful basis for the collection and the use of Personal Data;

(ii) Inform the individual that the Personal Data will be used for marketing purposes;

(iii) Implement any appropriate safeguards; and

(iv) Satisfy other compliance duties under any other relevant regulations.

2.0 Direct Marketing

2.1 As with any processing of Personal Data, the Data Subjects must be informed that their Personal Data will be used for marketing purposes. Depending on the situation, this can be done in several ways, such as:

(i) Referring to PETRONAS' privacy notice;

(ii) When collecting material online, by using pop-ups or links which provide information; and

(iii) Including specific information in the marketing materials that are sent out.

2.2 It is a good practice to make sure that the relevant privacy notice is broad enough to cover the activities mentioned in a particular direct marketing campaign before it is launched. If it is not broad enough, it is still possible to use the Personal Data, provided the recipients of the marketing communications are adequately informed in advance of the intent to use their data for the marketing purposes at issue and, where required, collect their consent.

Don't forget!

Don't send direct marketing messages without checking if any local laws may apply in your jurisdiction.

For example, in some jurisdictions, direct marketing activities must have opt-out option, as well as restrictions on volume and frequency of messages.

3.0 Opt-In (Affirmative Consent) and Opt-Out (Right to Object) on Marketing Matters

3.1 Depending on the jurisdiction, marketing rules may require that the affirmative consent of the recipient (i.e., "opt-in") be collected prior to sending him/her direct marketing material, even in a business-to-business context. The marketing team should consult LCD to determine whether it is necessary to launch campaigns to collect consent of contacts in certain countries prior to sending them direct marketing material.

3.2 Regardless of whether such "opt-in" is required, be mindful that it is necessary to provide a simple (and free of charge) way of "opting out" which is as simple as the "opt-in" on all direct marketing communications sent out, whether by fax, mail, e-mail or SMS, or through cookies or similar technologies (for example, a link to an opt-out page or a number to which a Data Subject may send a text message).

3.3 The Data Subject's right to opt out should be brought to their attention, at the latest, when the first direct marketing communication is made. The Data Subject's right to opt-out must be presented to them clearly and separately from any other information.

3.4 If a Data Subject opts out of unsolicited marketing communications, please ensure that:

(i) The opt-out request is processed in a timely manner;

(ii) This request or choice is recorded in the database entry that relates to the Data Subject. Simply deleting the Personal Data is not sufficient and may create problems as there will be no record of the Data Subject's choice for the future, even if the Data Subject's contact details are obtained again through another source; and

(iii) Unsolicited direct marketing material is not sent to the Data Subject again.

4.0 Online Behavioural Advertising ("OBA")

4.1 Company may undertake OBA to deliver targeted communications to a specific individual. For instance, company may utilise website advertising to observe an individual's interest online such as their frequently visited websites and location to deliver specific communication.

4.2 If company undertakes OBA, the following must be taken into consideration, as well as any other local requirements:

(i) Consent must be obtained before cookies can be used to store or access individual's personal data.

(ii) The consent must be specific, freely given and revocable. It requires active participation of Data Subject to Opt-In to provide valid consent, with the option to "opt-out" from subsequent processing.

Section 10: Employee Personal Data

1.0 Lawful Basis for Processing Employee Personal Data

1.1 Employers collect employee Personal Data for various purposes, for example to comply with law; to assist in selection for employment, training and promotion; to ensure personnel safety and security; amongst others.

1.2 The following are lawful bases for processing employee Personal Data:

(i) **The employee has given consent**

Consent is an appropriate and valid legal basis for collection of employee Personal Data in many countries globally. However, be mindful that in some jurisdictions such as the EU, it is specifically provided that the legal basis for collection of employee Personal Data should not be consent due to imbalance in power in the employer-employee relationship. In these circumstances, the employee is considered to not have genuine free choice to freely provide consent due to the imbalanced relationship and an alternative legal basis is recommended.

(ii) **Processing is necessary in fulfilling employment contracts**

The employment contract may include a provision which allows the employer to process the employee's Personal Data for the purpose of employment. This may include processing the employee's name and bank details for the purpose of providing salary.

(iii) **Compliance with legal obligations**

Employers may need to process specific information on its employees to comply with legal obligations, such as providing details of the employee's salaries to the local tax authorities.

(iv) **Processing is necessary for the employer's legitimate interest**

In jurisdictions where legitimate interests is a lawful basis for processing, the employer may be able to rely on legitimate interests in processing the employee's Personal Data if the legitimate interests test as per the Section 4 above is satisfied. For example, employers could have a legitimate interest to process employee Personal Data as part of an internal HR system upgrade for the purpose of providing better employment services to the employees.

2.0 Privacy Notice to Employees

2.1 A Privacy Notice must generally be provided to the employee, stipulating the processing of the employee's Personal Data as per Section 4 on Privacy Notice above.

2.2 Employees must be updated on any changes to the processing, including if there are any new purpose of processing that is relied on by the organisation.

2.3 The Employee privacy notice must provide the appropriate level of detail so that the employee can understand the purpose of processing, lawful basis that is relied on, recipients of their data, and whom they should contact if they have any queries on the above.

3.0 Retention Period

3.1 Employee records that are collected and processed should not be retained longer than required by the company or to comply with legal obligations.

3.2 For example, employee records should be deleted once the relevant employee resigns. However, in some countries, there are obligations under the employment laws to keep information registers of employees for a period of not less than six years.

3.3 Access to Personal Data of ex-employees retained due to any legal obligations should be limited on a need-to-know basis as it is unlikely for the information to be processed daily.

4.0 Employee Monitoring

4.1 In order to protect company confidential information as well as Personal Data from threat of loss, most companies use data loss prevention tools or technologies. These tools may be operated via systems and networks used by employees, such as email exchange servers. Proper safeguards must be put in place to ensure that the monitoring via data loss prevention tools is not excessive.

4.2 An employer must provide sufficient information to employees regarding the collection of these types or other monitoring activities in accordance with the requirements of the local jurisdiction where the company operates.

4.3 Data protection issues may arise when employees are allowed to use their own devices ("Bring Your Own Device" or "BYOD") for business communication purpose, such as integrating the work email to an employee's personal mobile phone.

4.4 The employee's privacy rights need to be balanced against the rights of the employer to protect business information. Additionally, the employer remains responsible as Data Controller in the processing of the employee's Personal Data and any other Personal Data transmitted using the work email setting.

4.5 Therefore the following should be considered by the organisation:

(i) Establish a policy or guidelines to inform employees of their responsibilities in using PETRONAS' information on their personal device;

(ii) Provide clarity on the measures taken by organisation in protecting PETRONAS' information; and

(iii) Put in place employee data management practices in the event the employee leaves the PETRONAS Group, or when the device is stolen or lost.

Don't forget!

Don't implement any software or tools with any employee monitoring without checking local law requirements –

these may include protection of personal data as well as employment law.

5.0 Local Requirements

5.1 Data protection issues may arise throughout the employment cycle, for example as follows:

(i) During the pre-employment period, a company may need to conduct background checks to potential employees;

(ii) During employment period, a company may need to conduct drugs and alcohol testing on employees, obtain specific health data such as vaccination status, address and manage diversity and inclusion issues, video surveilance and geolocation; or

(iii) Post employment, where a company may provide references to ex-employees.

5.2 As PETRONAS operates in various jurisdictions and may be subjected to various local personal data protection laws, there may be significant differences in managing the above issues pursuant to local requirements.

5.3 Therefore, the HR practitioners must be aware of the ever changing laws when managing and processing employees' Personal Data.

Section 11: Biometric Data

1.0 Managing Biometric Data

1.1 Biometric data refers to physical, psychological, or behavioural characteristics of an individual, which allows or confirms the unique identification of that natural person, such as facial images, fingerprints, handwriting, and voice.

1.2 Some jurisdictions such as the GDPR categorise Biometric Data as Sensitive Personal Data and require special precautions to prevent harming Data Subjects.

1.3 The use of biometric data is expected to grow with the advancement of technology.

1.4 Organisations may deploy systems that collect biometric data for verification and identification purposes, such as:

(i) **Verification**

An individual presents his passport and a sensor captures his biometric samples such as his face or fingerprint. This allows the system to create a biometric template to match the biometric samples provided against the passport.

(ii) **Identification**

An employee's biometric template such as his face has been stored in the access control system which allows the employee to enter the work premise when the camera captures the employee's facial image.

1.5 Data protection issues may arise when processing biometric data. For instance:

(i) **Identity spoofing**

The use of a synthetic object such as a synthetic fingerprint or a 3D model of a face to fake the physical characteristics of an individual in order to obtain a positive match in the biometric system.

(ii) **Error in identification**

As biometric systems rely on probabilistic matching, there is the possibility of a failure to identify an individual (false negative) when the threshold for matching is set too high, or wrongly identifying another person as the individual (false positive) when the threshold is set too low.

(iii) **Systemic risks to biometric templates**

The uniqueness of the biometric template declines if the same template is used across several different implementations, prompting access to the threat actor.

2.0 Considerations in Processing Biometric Data

2.1 Use of biometric data requires special precautions to prevent harming the Data Subjects.

2.2 In utilising biometric data as part of processing activities, please consider the following:

(i) Ensure lawfulness of processing Data Subjects' biometric data and where applicable, consent is obtained.

(ii) Minimise the storing of biometric data in the system and to discard the biometric samples as soon as practicable.

(iii) Implementing relevant security safeguards such as encryption of biometric templates and access and control measures to prevent unauthorised access.

(iv) Ensure biometric data is permanently deleted if it is no longer required or when the system is decommissioned.

(v) Carry out DPIA prior to processing biometric data if the processing is likely to result in a high risk to rights and freedom of individuals.

2.3 This consideration must be regularly reviewed to ensure compliance with relevant data protection regulations.

Contact Us

In the event of any doubts or questions concerning the application or interpretation of these Guidelines, please seek advice from the LCD of Group Legal.

Appendix I: Master Guidelines Checklist

NOTE:

This checklist is intended only as a general guide to facilitate PETRONAS OPUs/HCUs in assessing the level of personal data protection and privacy compliance in accordance with these Guidelines. Where applicable, it is your responsibility to adapt the checklist to suit the business and operations of your OPU/HCU, and to take into account the applicable personal data protection and privacy laws of your jurisdiction. Please do not regard this checklist as a comprehensive checklist to conclusively indicate your OPU's/HCU's compliance with the applicable personal data protection and privacy laws of your jurisdiction. Kindly read through the primary source of this checklist, i.e. these Guidelines, as well as the applicable personal data protection and privacy laws in respect of any legal points. This checklist was prepared in accordance with general law as at the version date of this checklist and has not been updated unless otherwise indicated. You must therefore check whether there are any specific local law requirements or whether there have been any changes in the law or practice since the date it was created or last amended.

In the event of any doubt or questions concerning the application or interpretation of this checklist, please seek advice from the LCD of Group Legal.

Personal Data Protection Principle	Checklist Items	Remarks
Collection of Personal Data		
Collection of data (consider both analogic (manual) and electronic data)	Collection of personal data adequate (and not excessive) Example: HR collects data fields as follows: • Name • Age • Address	
	Does the company process personal data of children? If so, consider how to obtain valid consent.	
Personal Data Protection Principle		
	Has there been appropriate measures to ensure only necessary personal data collected? Is the personal data collected accurate? Should/can data fields be anonymised/pseudonymised?	

Consent Principle	Obtaining consent – Customers Example: For customers, where applicable, consent is obtained via service agreement. [or to state if any other legal basis under the law applies: • Contractual Necessity • Legal Obligation • Vital Interests • Public Interests • Legitimate Interests]	
	Consent – Employees* • Is the processing necessary in the context of the performance of the employment contract (or to comply with legal obligations in this context)? *note consent is not a suitable legal basis for collection of employee personal data in the EU under GDPR.	State if exemption applies for seeking consent e.g EU countries
	Consent – Vendors, Suppliers, etc. Is the processing necessary in the context of the performance of the contract (or to comply with legal obligations in this context)?	
	Are records of consent maintained?	
Where the ground for processing is consent	Was the consent freely given and informed?	
	Was the consent presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form and using clear and plain language?	
	Does the data subject have the ability to withdraw his/her consent?	

Notice Principle	Have data subjects been provided with a privacy notice? Examples: • Privacy Notice for Customers • Privacy Notice for Employees • Privacy Notice for Vendors, Suppliers, Third Party Service Providers • CCTV Notice/Signage	
	Has the privacy notice been provided to data subjects whose data is collected directly from them before the processing starts?	
	If the data was received from a third party, has our privacy notice been provided within a reasonable period?	
	Is the language concise, transparent, intelligible and in an easily accessible form, using clear and plain language?	
Disclosure Principle	Disclosure only to third parties listed in Privacy Notice	
	Are there other disclosures? If yes – has consent been obtained?	
	List of disclosures to third parties	

Management and Control of Personal Data		
Security Principle	Is there a security policy?	
	Adequate security measures: • Password-protection and encryption for databases • Limit access to databases • Regularly change passwords • Regularly back-up databases • Limit remote access to databases (unless strictly necessary) • Limit access to physical personal data systems (e.g. file cabinets) • Ensure third party processors comply with appropriate security obligations; enter contracts with third party processors • Obtain assurance from cloud providers on security of cloud network and services • Anonymisation/ pseudonymisation (if possible)	
Accuracy Principle	Practical steps to ensure accuracy of personal data collected. For example: Send regular emails to employee to request for any updates (e.g. GHRM through MyCareerX)	
	Additional security requirements? (based on local applicable laws)	

Purpose limitation Principle	Is there a legitimate reason for collecting the personal data?	
	Has the purpose for processing been clearly identified from the start?	
	Where required, have they been notified to the individuals?	
	Will the personal data be used for a new purpose that is not compatible with the original purpose? If yes – obtain specific consent for the new purpose.	
Retention Principle	Is there a retention policy? (i.e. retention periods determined for storage of personal data)	
	Is there proper disposal of personal data?	
	Is a disposal schedule maintained?	
	Additional retention requirements? (based on local applicable laws)	
Access and Correction Principle	Disclosure only to third parties listed in privacy notice	
	Are there other disclosures? If yes – have the data subjects been informed? What legal basis applies to the disclosure?	
	List of disclosures to third parties	
Privacy by design and Privacy by default	Has the company assessed if DPIA is required and if so undertaken DPIA?	

Data Subjects' Rights		
Data Subjects Rights	Does the company enable employees and customers to exercise their rights as described in Section 7 of these Guidelines?	
	Does the company have the processes or technology to enable data subjects to exercise their rights?	
Outsourcing Data Processing Operations/Data Processors		
Data processors	Are there data processors? If yes, see below.	
	Are there written contracts entered into with the data processors?	
	Are there sufficient security obligations imposed on the data processors?	
	Are there sufficient guarantees obtained from the data processors as to the security of personal data?	
Transferring Personal Data In Different Countries		
Transfer of Personal Data abroad	Are there transfers of personal data outside of the jurisdiction? If yes, see below.	
	Which of the approved transfer mechanisms, applicable under each law, are used? Not exhaustive examples: • standard contractual clauses • consent of the data subject	
Data Breaches		
Data Breaches	Does the company have a data breach policy in order to identify the procedures to follow when a breach occurs?	

Direct Marketing		
Direct marketing	Are there direct marketing activities? If yes, see below.	
	Has consent been obtained from data subjects for marketing activities?	
	Is there an opt-out option provided to the data subjects?	
	Do-Not-Call/No-Marketing Registry	
Organisational and Security Measures		
Security measures	Are security measures appropriate for the personal data? Organisations can take into account the state of art, the costs and the nature, scope and context of processing in order to determine what is appropriate to the risks involved. Security covers organisational (e.g., people and processes) and technical measures. The following factors should be considered: • Pseudonymisation • Encryption • Ensuring ongoing integrity, confidentiality, availability and resiliency • The ability to restore in a timely manner • Processes for testing security	

Other Important Data Protection Requirements		
Registration as Data Users*	PDPA certificate of registration (where applicable) *	
	Display of certificate on the premises*	
Miscellaneous	DPO (where applicable)	
	Regular training of staff on personal data protection and privacy compliance	
	Personal Data Compliance Manual	
	Website Cookie Policy	

*Items specifically required under Malaysian Personal Data Protection Act 2010 ("PDPA")

Appendix II: Personal Data Protection Compliance Clauses

(As at June 2021)

Appendix III: Template of PETRONAS Privacy Notices

Appendix IV: Checklist to Develop and Monitor Personal Data Protection Training Programmes

Expectations		Elements/Metrics	Main Considerations
A) All Staff Training Programme	1.	The personal data protection & privacy training programme incorporates national and sector-specific requirements.	Are employee data protection training needs met? Have trainers received appropriate training?
	2.	The programme is comprehensive and includes training for all employees on key areas of data protection such as: a. Importance of personal data protection b. PETRONAS' Personal Data Protection Policies c. Main data protection obligations under the law including: i. Handling requests, ii. Data sharing, iii. Information security, iv. Personal data breaches and v. Records management.	
	3.	Consider the training needs of all employees and use this information to compile the training programme.	
	4.	Assign responsibilities for managing data protection and information governance training across the organisation and have training plans or strategies in place to meet training needs within agreed timescales.	
	5.	Have dedicated and trained resources available to deliver training to all employees.	
	6.	Regularly review the programme to make sure that it remains accurate and up to date.	
	7.	Senior management sign-off for training programme.	

Expectations		Elements/Metrics	Main Considerations
B) Induction and Refresher Training	1.	Appropriate employee, such as the DPO for the OPU or an information governance manager, oversee or approve induction training.	Can the training delivery methods be observed by regulators? Is the effectiveness of the training method measured? Does the company follow up on 'no shows'? Could employee explain their training records?
	2.	Employees receive induction and refresher training, regardless of how long they will be working for your organisation, their contractual status or grade.	
	3.	Employees receive induction training prior to accessing personal data and within a reasonable period from their start date.	
	4.	Employees complete refresher training at appropriate intervals (consider obligations imposed by regulators e.g., in their breach notification forms) or ad-hoc when there are relevant revisions to the personal data protection laws or regulations	
C) Specialised Roles	1.	Complete a training needs analysis for data protection and information governance employees to inform the training plan and to make sure it is specific to the individual's responsibilities.	Would an employee consider that there training needs have been specifically identified? Are there appropriate plans to meet those needs? Are the training materials effective?
	2.	Set out training and skills requirements in job descriptions of employees handling personal data.	
	3.	Keep evidence to confirm that key roles complete up-to-date and appropriate specialised training and professional development, and that they receive proportionate refresher training.	
	4.	Keep on record copies of the training material provided as well as details of who receive the training.	

Expectations		Elements/Metrics	Main Considerations
D) Monitoring	1.	Conduct an assessment at the end of the training to test employee understanding and make sure that it is effective, which could include a minimum pass mark.	Do employees react positively to the training? Is there an easy way to provide feedback? Does that process result in changes? Are senior managers aware of training monitoring outcomes?
	2.	Monitor training completion in line with organisational requirements at all levels of the organisation and follow up with employees who do not complete the training.	
	3.	Employees are able to provide feedback on the training they receive.	
	4.	Regularly uses a variety of appropriate methods to raise employee awareness and the profile of data protection and information governance, for example, by emails, team briefings and meetings, posters, handouts, and blogs.	
	5.	Make it easy for employees to access relevant material and find out who to contact if they have any queries relating to data protection and information governance.	

Appendix V: Guide to Handling Data Subject Access Request

Guide to Handling Data Subject Access Requests

Purpose of These Guidance Notes

1. This guide aims to help effectively manage individuals' requests for access to their personal data in compliance with applicable laws.

2. These guidance notes to be read with the Master Guidelines to the PETRONAS Corporate Privacy Policy on key concepts of personal data, access requests, in particular the chapter on data subject rights, as well as any other relevant guidelines issued under the applicable local laws from time to time.

3. The template provided herein are for guidance purposes only. OPUs should evaluate their own requirements in light of their obligations under local laws and organisation structure and customise the forms accordingly. It should not be assumed that following these sample templates would mean compliance with local laws, particularly where they may be updated from time to time.

Access Obligation

1. On request by an individual, an obligation commences to provide, as soon as reasonably possible and no later than any deadline imposed by applicable privacy legislation:

    a. Confirmation of whether or not the individual's Personal Data are being processed;

    b. Access to Personal Data about the individual that is in the possession or under the control the company; and

    c. Information about the processing itself such as purpose of processing, categories of data and recipient, duration of processing, data subject rights and appropriate safeguards in case of third-party transfer;
    unless there are any exceptions or prohibitions to providing the information.

2. Example:

    Eddy request for personal data relating to him during the course of a legal proceedings or lawsuit. However, the applicable local laws (e.g., laws which governs employment relations) contain certain provisions which limits the scope of information to be provided or exchanged between parties to an ongoing legal proceeding. In this context, Eddy may not be entitled to receive more information than prescribed by that local law.

3. The purpose and aim of right of access is to enable a person to have control over Personal Data relating to them that it allows them to "be aware of and verify the lawfulness of the processing".

4. The different types of requests that can be made by an individual include the following (depending on jurisdiction):

    a. Reasons why the Personal Data is held or processed;

    b. Description of the Personal Data concerning the individual;

    c. Who has received or will receive their Personal Data;

    d. Details of the source of the Personal Data if it was not collected from them;

    e. Period for which their Personal Data will be stored;

    f. Rectification, erasure portability or objection to profiling of Personal Data;

    g. Logic of automated profiling of Personal Data (if any); and/or

    h. Details of cross border transfer of their Personal Data (if any).

General Principles of Right of Access

1. Depending on the requirements under applicable law, the general principles under the right to access include:

   a. **Completeness of information**

      All Personal Data requested should be provided unless there is an exception.

   b. **Correctness of information**

      All actual information to be provided including data which are inaccurate or where the processing may no longer be lawful.

      Example:

      A company discovers in responding to an access request, that an applicant's resume was stored beyond the retention schedule. n this case, the company cannot first delete the information and then reply that there is no data on the application. It first has to give access and then delete the data afterward. To prevent subsequent requests for erasure, it is recommended that the company record the fact and time of erasure.

   c. **Time reference point of assessment**

      There is an obligation to provide Personal Data which is available. Personal Data which have been processed in the past but may have been disposed of based on the retention policy is not required to be provided.

d. **Comply with data security requirements**

Communication and providing access to Personal Data is a data processing activity. Therefore, it continues to be necessary to ensure the security of the Personal Data by implementing appropriate technical and organisational measures to protect the Personal Data.

Example:

i. **Responses by mail**

Consider secure mail delivery, e.g., registered mail or offer for the document to be collected with signature of receipt from the OPU's premises.

ii. **Responses by electronic means**

Apply appropriate levels of security, e.g., encryption or password protection when sending the data.

2. The process flow for responding to a Data Subject Access Request is included below.

1	Gather all required information	To ask for sufficient additional information to assist with the request, if required.
2	Analyse the request	To contact the relevant department/ authorised personnel to analyse and prepare response to the request.
3	Act on the request	To act in accordance with a justified request. May consider denying or refuse the request with proper justification, which needs to be provided to the Data Subject.
4	Communicate within timelines	Communicate within the defined timelines: 1. Acknowledgment of the request – as soon as practicable. 2. Response to the request – within the timeframe provided under the law.

[Note: See sample responses in Annex C]

Process for Responding to Access Requests

The following steps are to be taken to ensure that a company is in a position to comply with an access request:

A. Receiving an Access Request

A1. Making access request channels available

- Provide appropriate user-friendly communication channels to allow a person to submit an access request. For example, provide the contacts to which a data subject access request may be submitted in person, through email or post. This is usually in the privacy notice. Please refer to Annex A for a sample access request form.

- If the Personal Data requested can be retrieved by the individual himself/herself, provide clear information on how this can be done. For example, the individual can log into his/her online account to access their personal data.

A2. Log the access requests

- Keep a record of all access requests received and processed, documenting clearly whether the requested access was provided or rejected. Proper documentation will help in the event of a dispute or an inquiry by the regulator. As part of the documentation process, consider using an acknowledgement form (please see Annex B for a sample acknowledgement form).

- Additionally, put in place an appropriate retention policy for the keeping of such records, including the duration for which they will be retained. Stop retaining records containing the individuals' Personal Data where retention is no longer necessary for any legal or business purposes.

B. Validate the Request

The following are the 3 main queries

- Is the information on the **identity** of the requester complete?
- Is the nature or extent of the **request clear**?
- Is the requester **authorised** to act on behalf of the data subject?

Don't forget!

Don't forget when validating a data acces request, to check whether there are any local law exceptions that may require PETRONAS to reject or choose not to comply with such request.

For example, in most jurisdictions, personal data which is subject to legal privilege will not be required to be provided as part of an access request.

B1. Ascertaining identity

- Conduct verification when processing access requests (e.g., verification questions to be asked to establish the identity of the requestor).
- In undertaking this exercise ensure that Personal Data collected is limited to those necessary to enable identification of the individual and no more.
- Where appropriate, implement an authentication (verification of identity) procedure throughout the process of handling Personal Data.

Example:

Amina has created an account in the online store, providing her e-mail and username. Subsequently, Amina asks the OPU for information whether it processes her Personal Data, and if so, asks for access. OPU requests Amina's ID to confirm her identity. OPU's action in this case is disproportionate and leads to unnecessary data collection. Instead OPU can ask (non-intrusive) security questions that were configured when she registered her account or employ multifactor authentication for access requests.

B2. Clarify request

- Unless explicitly stated otherwise under local law or any exceptions apply, the legal obligation is to provide ALL Personal Data concerning the individual. Access to Personal Data means access to the actual Personal Data itself, not a general description or reference to categories of Personal Data processed by the company.

- The right of access also includes information on processing activity of that Personal Data which can be based on privacy notice provided to the data subject.

- However, the individual can be requested to specify the request if PETRONAS processes a large amount of data about the individual.

- Analysis of the content of the request

a. Does it concern other Personal Data or other company information e.g., name of a vehicle or vessel will not be Personal Data; and

b. Is the request related to the requesting person (or a person authorised to make the request)?

Example 1:

A company receives a general access request by letter from a long-time customer. Even though deletion periods are fully respected, the company processes a vast amount of data concerning the customer, because processing is still necessary to fulfil contractual obligations arising from the contractual relationship with the individual (including for example continuing obligations, communication on controversial issues with the customer and with third parties) or to comply with legal obligations (archived data that have to be stored for tax purposes, etc.).

The company may have doubts as to whether the request, that was made in very general terms, is really intended to encompass all kinds of those data. This may be especially problematic if the request is to be sent to a postal address of the person and therefore has to be on paper.

The company may request that the person specify the type of Personal Data requested and provide the date and time the Personal Data was collected, as this would help narrow down the search to provide the information requested.

Example 2:

A company receives a request for access to the Personal Data from the person who claims to have been recorded by the company's video surveillance. The company actions will depend on the additional information provided. If the requesting person indicates a particular day and time when the cameras may have recorded the event in question, it is likely that the company will be able to provide such data. However, if the request concerns e.g., a year of recordings, the company who is unable to process such a large amount of data may refuse to take action due to not being in the position to identify the person concerned.

Example 3:

Ali was provided a permanent parking space by his OPU. However, when he arrives for work, another car is parked in his parking lot. Since this situation is repetitive, Ali asks the OPU security to view the video surveillance system covering the office's parking lot area, for access to the Personal Data of this driver. In such a case, Ali's request will not be a request for access to his Personal Data, as the request does not concern his Personal Data but actually the data of another person. Therefore, this should not be considered a data subject access request.

Don't forget!

Don't disclose any personal data without verifying the identity of the person making the access request.

B3. Ensure requester is authorised

- If the requestor is making an access request on behalf of another individual, ensure the requestor is legally authorised to act on behalf of the individual.

Example 1:

A shop receives a request from Person A to view CCTV footage of Person B's visit to the shop at a specific time and date. Person A provides sufficient information to the shop to determine when Person B visited the shop. Person A identifies themselves to be a friend of Person B and indicates that they are acting on behalf of Person B who misplaced their wallet while in the shop. The shop may ensure that Person A is legally authorised to act on behalf of Person B by requesting for evidence such as a signed letter from Person B consenting to or authorising Person A to request for their Personal Data on their behalf.

- If an access request from two or more individuals (e.g., husband and wife) for their respective Personal Data captured in the same set of records was received, consent will need to be obtained from the respective individuals to disclose their personal data to each other. Once obtained, the couple can be provided access to a common data set containing their Personal Data, without having to exclude the Personal Data of the other individuals. If such consent cannot be obtained, access to the individuals' data should be provided separately, for example, by masking the Personal Data of the other individuals before providing the individual access to his own Personal Data, and vice versa.

- Additional care is required when dealing with access requests from minors to ensure that the best interest of the child is protected. Note that local laws may provide for parental responsibility to ask and receive information on their child e.g., performance in educational institution.

- In addition, always consider if there are other prohibitions or exceptions to providing access that would apply.

B4. Validate the request

There may be circumstances where the OPU does not need to provide access to the Personal Data requested based on local laws . Take into consideration the following:

- The request should not affect the rights and freedom of others or result in the company having to violate its legal or statutory rights;
- The request should not have negative impact on national security, public security, defense or challenge any criminal conviction on the data subject; and
- Data pertaining to occupational health to be checked with Group Health Safety Security and Environment (GHSSE).

Example 1:

An individual makes a claim to the company for compensation for slipping on the staircase while at the office. The company disputes the amount of compensation they should pay. An internal paper briefing the company's senior management sets out the maximum sum the company is willing to pay to avoid the claim going to court. If the individual makes an access request to the company, the internal paper will not need to be provided as doing so would be likely to prejudice any negotiations to settle the claim.

Example 2:

Aminah lodges access requests every two months with the carpenter that manufactured her a table. The carpenter answered the first request completely. When deciding whether a reasonable interval has elapsed, one should consider that the carpenter only occasionally and not as part of its core activity processes and collects Personal Data and it is even less likely that the carpenter often provides services to the same data subject.

Indeed, the carpenter only manufactured the table and did not provide any more service to Aminah, hence it is unlikely that changes occurred in the dataset concerning Aminah. Also, given the nature and amount of the Personal Data processed, the risks related to the processing can be considered to be relatively low as the purpose of the processing (i.e. billing purposes and compliance with obligation to keep records) is not likely to cause detriment to Aminah. The request furthermore concerns the same information as the last request. Such requests may therefore be regarded as excessive due to their repetitive nature.

- When assessing whether any exceptions or prohibitions apply, consider if it is possible to provide the individual with the requested Personal Data or information without the Personal Data or information excluded. If that can be done, then the individual should be provided access to the Personal Data without the Personal Data or information excluded. For example, if Personal Data requested by the individual also contains Personal Data of another individual, and it is possible to mask out the Personal Data of the other individual, the access to the requested Personal Data must be provided without the Personal Data of the other individual.

- If any exception or prohibition under the law applies such that the access request may be rejected, as good practice, inform the individual of the relevant reason(s) so that the individual understands the reason(s) behind the decision. See example response in **Annex C**.

C. Preserving Personal Data

Preservation of personal data may occur in any of the following situations:

- While processing an access request
- After rejecting an access request

While processing an access request

- When an access request is received, locate the requested Personal Data as soon as reasonably possible, and ensure the requested Personal Data is preserved while the access request is being processed.
- However, do not unnecessarily preserve Personal Data "just in case" of possible access requests. Personal Data should only be retained when there are business or legal purposes to do so.

After rejecting an access request

- Should an access request be rejected, continue to preserve the requested Personal Data for a reasonable period (minimally 30 days) after rejecting the request.
- In the event the individual submits an application to the regulators to review the rejection of the access request, continue to preserve the requested Personal Data until the review is concluded and any right of the individual to apply for reconsideration and appeal is exhausted.

Annex A: Sample Access Request Form

[Note: This needs to be tailored to local law requirements.]

Application to Access Personal Data	
1. Under personal data protection laws, you are entitled to request for your personal data that we have, and request to know how your personal data has been used or disclosed. 2. Please complete this form and submit it to: <Please specify any other modes to submit an access request below> In person or by post: [Data Protection Officer Organisation ABC ABC Complex 123, ABC Road] Alternatively, you can email the completed form to us: [DPO@abc.com]	
Particulars of Requestor	
<For this section, please determine the types of information you required in order to process the access request, including any documentation required to establish that the requestor is legally authorised to act on behalf the other individual(s)>	
Name of requestor:	
Contact number:	Email address:
Please check the applicable box(es): ☐ I am making an access request for my own personal data ☐ I am making an access request on behalf of other individual(s)	
Please complete this section if you are making an access request on behalf of other individual(s)	
Name of other individual(s) whom you are making an access request on behalf of:	
Contact number:	Email address:
Description of the Personal Data Requested	
To enable us to process your access request quickly and efficiently, please provide us with as much information as possible about the personal data you are requesting access to (e.g., type of personal data, date, time).	

Declaration	
By submitting this form, I confirm that the information stated above is true, complete and accurate to the best of my knowledge and belief.	
_____ Name & signature	_____ Date (DD/MM/YYYY)

<Proof of identity>

- If an individual is making an access request for his/her own personal data, please ensure the individual provides proof of identity or documentation to assist with the request. Do note that the proof of identity or documentation may vary depending on the nature and type of the request.

- For example, if individual request an access to his personal data in the service that it subscribed to, consider requesting for the name, membership number or any other information that can support the verification.

- If the applicant is making an access request on behalf of another individual, an authorisation letter/form should be presented for verification purpose.

<Processing>

- Please make clear the processing time for an access request and inform the individual if the business requires more time to process the access request, subject to the requirement under the law.

<Denial of access request>

- Please make clear if there are any circumstances where we cannot grant an access request. For example, prohibitions or exceptions that are provided under local privacy laws or other written laws.

Annex B: Sample Acknowledgement Form

Acknowledgement of personal data received for an access request

References number:
Name of Recipient:
Contact details:

No.	Document/Material	Data Received
1		
2		
3		
4		
5		

Signature of Recipient	**Date** (DD/MM/YYYY)

For internal use only	
Person in charge in handling access request:	
Date:	Time:

Annex C: Other Templates of Communication

Sample Responses to Data Subject

Dear [Requestor's Name],

[SAMPLE 1 – Sample Email verification]

Thank you for confirmation in the email below.

To effectively assist you in locating your data in our system and databases, appreciate if you could kindly provide the details as attached for us to assist you further with your request.

[SAMPLE 2 – OPUs/HCUs require more time to process the request
(Note: subject to time limit as specified by relevant jurisdiction, e.g., Malaysia PDPA - up to 14 days)]

Thank you for contacting PETRONAS. We hereby confirm that we have received your deletion request and are currently looking into fulfilling your request.

We are processing your request and will be updating you at our earliest convenience.

[SAMPLE 3 – Request for erasure – OPUs/HCUs sending confirmation to delete the requested information]

Thank you for contacting PETRONAS. We hereby confirm that we have received your deletion request. Our record indicates that we processed the following personal data which belongs to you:

Categories of Personal Data	*Purpose of Processing*	*Categories of Third Parties*	*List of Third Parties*

We will proceed to delete these personal data as per your request earlier.

[SAMPLE 4 – OPUs/HCUs deny or refuse the request to access or erasure of personal data with valid justification]

Thank you for contacting PETRONAS. We hereby confirm that we have received your deletion request. However, we are unable to proceed with your request due to the following:

[To inform justification to refuse deletion – as per S32 of PDPA, e.g., compliance with legal obligations, pending legal claims, etc.]

Thank you.

Passionate about Progress