PETRONAS

MASTER GUIDELINES

TO THE

PETRONAS CORPORATE PRIVACY POLICY

TABLE OF CONTENTS

These PETRONAS Master Guidelines ("Guidelines") is an operational document intended to compliment the PETRONAS Corporate Privacy Policy ("Corporate Privacy Policy") and intended to apply in all countries in which PETRONAS conduct operations. It does not describe all applicable laws or other policies of PETRONAS, or give full details on any particular law or policy. It does not constitute legal advice.

PETRONAS reserves the right to review and modify these Guidelines from time to time in compliance with the requirement of applicable law.

SECTION 1 - OVERVIEW

1. PETRONAS Corporate Privacy Policy

1.1. These Guidelines are prepared with a view to complement the Corporate Privacy Policy which sets out the broad principles governing personal data protection and privacy practices of PETRONAS (as defined in the Glossary).

1.2. The Corporate Privacy Policy provides that PETRONAS, in the collection, use, processing and storage (all of which are included as operations of "processing" under the applicable personal data protection and privacy laws, and as set out in the Glossary) of personal data, shall take the following steps where required to do so by applicable law, also known as our Core Principles:

- to obtain adequate consent from individuals ("**Consent Principle**");
- to provide individuals with the required notices and information, and verify that their personal data has been obtained lawfully and that it is relevant for the stated purposes ("**Notice Principle**");
- to keep accurate, complete and up-to-date the personal data that has been collected ("**Accuracy Principle**");
- to retain the personal data that has been collected only for the period necessary to fulfill the relevant purposes, unless otherwise permitted or required by applicable law ("**Retention Principle**");
- to inform individuals concerned about the disclosure of their personal data to third party recipients ("**Disclosure Principle**");
- to keep personal data secure by protecting it with adequate and appropriate security safeguards ("**Security Principle**"); and
- 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**").

1.3. These Guidelines are part of the PETRONAS' personal data protection and privacy compliance programme. It reflects the increasing need for effective personal data protection and privacy compliance measures in the conduct and business activities of PETRONAS group of companies domestically and worldwide.

1.4. Your compliance with and support for the letter and spirit of these Guidelines are vital to PETRONAS' continued success. Your failure to comply may have severe consequences for PETRONAS or PETRONAS group of companies and may result in disciplinary action against you.

1.5. In the event of any doubts or questions concerning the application or interpretation of these Guidelines, please seek advice from the Legal Compliance Department ("**LCD**") of Group Legal.

2. Application of these Guidelines

2.1. These Guidelines are intended to apply to PETRONAS (defined in the Glossary), as well as to every employee of every PETRONAS group of companies worldwide. It is also intended to apply to every director (executive and non-executive) of those companies. As an employee or director of PETRONAS and/or PETRONAS group of companies worldwide, you are responsible for reading, understanding and complying with these Guidelines.

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

2.3. Although these Guidelines are specifically written for PETRONAS employees and directors, PETRONAS encourages that its contractors, subcontractors, consultants, agents, representatives and others performing work or services for or on behalf of PETRONAS group of companies to comply with it in relevant part when performing such work or services. Failure by a contractor, sub-contractor, consultant, agent, representative or other service provider to comply with the principles and standards set out in these Guidelines may result in the termination of the non-complying party's relationship with PETRONAS and other adverse consequences.

2.4. "**We**", "**us**", "**our**", "**ours**" shall denote application of the requirement of these Guidelines to PETRONAS.

2.5. "**You**", "**your**", "**yours**" shall denote application of the requirement of these Guidelines to every employee, director, or such other category of individuals as made applicable in the context.

3. Purpose of these Guidelines

3.1. These Guidelines provide you with an overview of the principles that apply within PETRONAS to the collection, use, processing, and storage of personal data about any individuals (whether personal data of customers, employees, suppliers, service providers, business partners, etc) (for ease of reference, "**Guideline Principles**"). Its purpose is to ensure that the flow of personal data we manage every day is processed as safely as possible, respecting individual rights to data protection and privacy, and in compliance with applicable personal data protection and privacy laws.

3.2. These Guideline Principles have taken into account the Core Principles in the Corporate Privacy Policy, and best practices based on the personal data protection and privacy laws of most jurisdictions.

3.3. These Guideline Principles should be followed and practised in the everyday collection, use, processing, and storage of personal data by PETRONAS, which are briefly summarised in the following applicable situation/scenario:

- when collecting personal data - see Section 2;
- when managing and controlling of personal data -see Section 3;
- when handling enquiries and responding to requests from individuals regarding their personal data - see Section 4;
- when setting up outsourcing services in relation to such personal data - see Section 5;
- when exporting personal data to another jurisdiction - see Section 6; and
- when using the personal data collected for the purpose of marketing - Section 7.

3.4. You must also take into account and comply with any prescriptive, additional and/or specific personal data protection and privacy requirements in accordance with the local personal data protection and privacy laws of the respective jurisdictions.

4. Basic rules to keep in mind

4.1. As an introduction to the concept of personal data protection and privacy, personal data protection and privacy rules are designed to generally ensure that:

- personal data is only used for the purposes for which it is provided;
- to grant individuals a certain degree of control over their personal data;
- to ensure personal data is not retained for longer than necessary;
- to ensure security for personal data including protection against, loss, damage, or destruction; and
- to ensure that personal data kept is accurate and updated.

4.2 The Core Principles as provided under the Corporate Privacy Policy and many of the Guideline Principles flow from the rules above.

4.3 Understanding the concepts and rules of the personal data protection and privacy issues and its applicability to your ordinary course of business operations from the data subject's perspective, will assist in reducing the chance of you infringing any applicable personal data protection and privacy law.

SECTION 2 - COLLECTION OF PERSONAL DATA

This section provides general information about the obligations to be complied with prior to collecting and processing personal data.

Guideline 1. Accountability

1.1. PETRONAS, as the "data controller" (as defined in the Glossary) of personal data, is accountable for the lawful processing of personal data. Regulatory authorities often have investigatory powers and can impose fines for violations of the applicable personal data protection and privacy laws.

1.2. The maximum fines which can be imposed under certain personal data protection and privacy laws are very severe. For example, the European Union General Data Protection Regulation ("GDPR") provides for administrative penalties of up to EUR 20 million or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

1.3. In order to ensure accountability over the processing of personal data, we should be guided by the following: -

I. Data protection by design and by default

(a) We must ensure that personal data protection and privacy requirements are placed at the forefront of our operations by design and are taken into account when putting in place the means by which we process personal data.

(b) We must ensure that we have the appropriate technical and organisational measures in place to ensure that, by default, we only process personal data to the extent it is necessary.

(c) We should design our database fields to enable us to quickly identify:

(i) the personal data we have collected;

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

(iii) whether it is necessary to retain the personal data for this purpose.

(d) We should build into our processes, appropriate mechanisms by which we obtain consent from data subjects and we retain a record of the scope of the consents provided.

(e) Additionally, we should also consider the following in our collection and processing of personal data:

(i) Data minimisation:

- Limiting personal data collected to what is adequate, relevant and necessary in relation to the purposes for which it is processed.

- Holding the minimum personal data necessary for our purposes. Consider the purpose for which you are collecting the personal data, and what is adequate, relevant and necessary to achieve that purpose. You should make the assessment separately for each individual on whom you hold personal data (or, where you are holding personal data on a group of individuals where the members of that group share relevant characteristics).

(ii) Accuracy:

- You should take every effort should be made to ensure that personal data is accurate and up to date.

- You should review the personal data stored and consider whether steps need to be taken to confirm its accuracy, or alternatively whether it should be rectified or erased.

(iii) Anonymisation/Pseudonymisation:

- There may be circumstances in which personal data can be processed so as to no longer allow attribution to a specific data subject (i.e. anonymisation or pseudonymisation).

- We should at all times consider whether it would be appropriate to apply anonymisation or pseudonymisation, based on the feasibility of anonymising or pseudonymising the personal data and the sensitivity of such personal data.

(f) Our accountability obligations will apply to all of our activities which involve the processing of personal data. Particular attention should be given to our three main categories of databases:

(i) Employee databases:

- This covers database for the hiring, payroll, career progression, notifications to tax administration, payment of social contributions, management of vehicles, payment cards, elections of employee representatives, IT network services and professional e-mails.

- These types of use are generally allowed under even the strictest personal data protection and privacy laws because they are necessary to allow PETRONAS group of companies to carry out their obligations to their employees. We are therefore generally not required to obtain our employees' consent. Please consult the LCD, of Group Legal if you need specific advisory on whether consent is required or not.

(ii) Marketing databases:

- This covers database for the client and prospective client, promotional and marketing, lead generation, web-based marketing, telemarketing and similar databases.

- Further details of what you can or cannot do for marketing database is provided in Section 7 of these Guidelines;

(iii) Customer invoicing/order processing databases:

- operations, quotations, invoicing, collection and after sales support.

1.4. These are just examples of personal data that we process, and are non-exhaustive. Please contact the LCD of Group Legal to discuss any additional categories of database.

II. Special care in respect of sensitive personal data

1.5. Where the personal data is "sensitive" (defined in the Glossary), we are required to take extra care to make sure that we have the data subject's express agreement before using it and that we take extra care when storing and/or transferring it.

1.6. Ideally, we will keep sensitive personal data separately so that it can be accessed and/or deleted independently of other personal data. At the very least we need to be able to identify it and control what it is used for.

1.7. We should also make sure that the personal data is relevant to the purpose for which it was collected, as various personal data protection and privacy laws do not permit us to store or process data that we do not need or which is not relevant to our business. This is particularly the case with sensitive personal data which very often we do not need and would therefore not routinely collect and store unless there was a specific reason for doing so.

III. Record keeping

1.8. We must maintain a record of processing activities to demonstrate compliance with the personal data protection and privacy requirements.

Guideline 2. Legal grounds and Lawful processing

I. Processing Personal Data

2.1. Personal data can only be processed where one of the following grounds applies:

(a) Consent from the data subject is obtained;

(b) Contractual necessity;

(c) Necessary to comply with legal obligations;

(d) Necessary to protect the data subject's vital interests;

(e) Necessary for the performance of tasks carried out in the public interest; or

(f) The data controller has a legitimate interest in processing the personal data, which is not overridden by the rights or freedoms of the data subject.

2.2. These are just examples of legal grounds, and are non-exhaustive. Please consult the LCD, of Group Legal for specific advisory where you are uncertain as to whether the collection and processing of personal data falls within any of the abovementioned legal grounds.

II. How Do You Obtain Consent?

2.3. As a general rule, you must obtain consent from individuals whose personal data you collect, unless any of the abovementioned legal grounds apply or where you can rely on any other exemption under the applicable personal data protection and privacy laws. Please refer to the LCD, of Group Legal for specific advisory if you are unsure.

2.4. Where consent is relied on, please note that the strictest personal data protection and privacy laws provide that such consent must be freely given, specific, informed and unambiguous.

2.5. In light of the emphasis on consent being "specific" and "unambiguous":

(a) Passive behaviours may not be acceptable under the strictest personal data protection regimes (i.e. where the data subject continues exploring a website despite a notice or banner which refers to the relevant privacy policy);

(b) Affirmative action is preferred and that includes, 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;

(c) It is important that we maintain a record that consent has been obtained so that we are in a position to demonstrate that consent was freely given.

2.6. While there is no particular form that consent must take, it must be a clear statement or other affirmative indication of the data subject's agreement to the collection and processing of his/her personal data.

2.7. The best time to obtain consent is when we collect the information, for example when a customer or job applicant fills in an online application. By using a standard privacy notice and opt-in/opt-out language we can inform individuals why we need the personal data and give them an opportunity either to limit or expand what we can use the personal data for. These topics are covered below.

III. Use of Privacy Statements

2.8. A Privacy statement explains how personal data of data subjects will be collected and used. This is an easy way of communicating with our data subjects what their information is being used for and how it will be processed. Data subjects can then read the privacy statement before deciding whether or not to provide the information.

2.9. It is therefore recommended to include a reference or link to our privacy statement on our marketing materials and other communications.

2.10. The privacy statement needs to be prepared in accordance with the requirement of personal data and privacy laws of the country.

IV. Opt-in/opt-out language

2.11. We may collect and use personal data for a variety of different purposes. That same personal data set may also be used to market products which a customer has already bought, or sell different products altogether. In these circumstances it may be appropriate to give the data subject a "shopping list" of types of processing which they can choose from. Opt-in/opt-out language is a good way of offering the data subject a way of deciding what is allowed and what is not.

2.12. In certain cases, there may be legal reasons why "opt-in language" (rather than opt-out) should be used; please check with the LCD, of Group Legal for specific advisory if in doubt.

2.13. Please also note that opt-ins are a way of showing that a data subject has expressly consented to having their personal data stored and processed by PETRONAS. For that reason, you cannot use "pre-ticked" boxes or other devices hoping that the data subject will not notice as this will not count as an opt-in.

SECTION 3 - MANAGEMENT AND CONTROL OF PERSONAL DATA

This section provides general information about the obligations to be complied with in the management and control of personal data.

Guideline 3. Database Fields

3.1. We need to have a good system for managing our personal data in an organised way.

3.2. We should control access to databases for security, manage personal data which are sensitive, respond quickly to data subject's requests, keep personal data up to date and delete it when it is no longer needed.

3.3. All PETRONAS group of companies storing personal data should have systems which allow them to meet these requirements.

3.4. We need to keep a "database of databases" so we know what data is kept where, by whom, for what purpose, and for how long.

Guideline 4. Database Security

4.1. Database security is a key issue, not only because data subjects expect it, but because of the risk of fines or other enforcement action from authorities in jurisdictions with strict personal data protection and privacy laws, in the event that we lose personal data or it is stolen from us.

4.2. The following security measures should be put in place and implemented (as necessary) across the PETRONAS group of companies to ensure the security of personal data:

(a) Password-protection and encryption for databases if transferred to laptops or portable storage devices to prevent unauthorised access.

(b) Access limited to people administering and/or using the database and only to the extent their access is required (on a need basis, i.e. no blanket access to a category of personnel).

(c) Passwords should be changed on a regular basis.

(d) Regular back-up of databases to prevent accidental loss or destruction.

(e) Limiting remote access to databases if this is not strictly necessary as it increases the risk of unauthorised access.

(f) Limiting access to physical data processing systems/ cabinets or filing systems containing information to authorized persons. This may involve measures such as secure premises and restricted access to rooms or storage areas. There must be strict authorisation as to who can deal with physical information marked for disposal.

(g) Ensure that any third parties who store personal data on our behalf comply with appropriate standards and sign a contract that contains contractual obligations to keep personal data safe.

(h) Seeking assurances from cloud suppliers about how personal data in the cloud will be kept safe, the security of the cloud network, and the systems in place to prevent hacking or disruption of access to the personal data. Physical security of our cloud providers data centres should also be checked.

(i) Anonymising/Pseudonymising personal data where possible.

(j) Regularly monitoring compliance with the above security measures, internally within PETRONAS organisation and also externally (i.e. third party service providers or data processors).

4.3. The security measures implemented must also take into account any additional and/or specific personal data protection and privacy requirements of the country.

Guideline 5. Updating and deleting database entry

5.1. Information contained in a database must be accurate and relevant. We are responsible for keeping the personal data we retain up to date and/or deleting them when they are no longer needed.

5.2. Practical steps to ensure the database entries are up to date includes:

(a) Provision of annual statements to data subjects setting out the information held on them, or

(b) Providing a method for checking personal data such as secure online access to data subject details on a website, and requesting updates, as relevant.

5.3. Practical steps to ensure the database entries are retained for as long as is required to achieve the purpose for which personal data were collected and are being processed includes:

(a) At the end of the standard retention period set for each database, or when a database entry becomes irrelevant, personal data should be reviewed and securely deleted if it is no longer required.

(b) In practical terms, physical, paper-based databases, should be reviewed regularly and entries that are no longer relevant (for example, because the employee is no longer with PETRONAS or any of its subsidiaries) should be destroyed. This information should be destroyed securely (shredded) and discarded in confidential papers bins and not in general bins.

(c) In relation to the paper-based databases sent to storage, you should make sure that any information you send to a storage facility is reviewed on a regular basis for the same purposes, or by agreeing on short destruction deadlines with the storage provider.

(d) As regards electronic databases, one way of ensuring that we review data at regular intervals is to set a "destroy by" date in a field in the database. Personal data that is not used by this date will be destroyed automatically. If we ever have to restore

databases from back-up tapes (which should also be kept only as necessary), we should also make sure that we delete all entries that are not useful anymore prior to using this database again.

(e) Standard retention periods should be reviewed regularly to ensure that we are not retaining any personal data that we no longer use and have an efficient means of marking, updating and securely deleting personal data as necessary and on demand.

(f) The same principles shall apply where a data subject invokes their rights under the personal data protection and privacy regime applicable to them, including for example their right to restriction of their personal data, or their right to rectification.

5.4. The standards of retention period should also take into account any additional and/or specific personal data protection and privacy requirements of the country.

SECTION 4 - HANDLING ENQUIRIES FROM DATA SUBJECTS

This section provides general information about the obligations to be complied with in handling enquiries from data subjects.

Guideline 6. Request for access to personal data

6.1. Data subjects may have rights over the personal data we hold about them. This allows them to keep some control over their information and to ask us to stop doing things that they do not like. Such rights may include:

(a) The right to request confirmation as to whether or not we are processing their personal data and are entitled to receive copies of any personal data we hold.

(b) The right to ask about the type of processing we do, the purpose of the processing, the source of personal data we hold (that is where we got it from) and any third parties with whom we share this information.

(c) The right to ask for how long their personal data will be stored.

(d) The right to request that we update and/or correct information about them when that information is obsolete or incorrect and the right to have their personal data deleted.

(e) 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.

(f) The right to be informed of any automated decision-making, including profiling used in connection with their personal data.

(g) The right to ask that we restrict the way in which we process their personal data.

6.2. It is possible to refuse to act on a request of a data subject (or charge a reasonable fee) if it can be demonstrated that such request is manifestly unfounded or excessive (in particular because of its repetitive character). In case of a suspicion that a request is frivolous or vexatious, such circumstances and related evidence should be sent to the LCD, of Group Legal to determine how to respond to such request.

Guideline 7. Manner and timing of response

7.1. Data subjects' enquiries may come in directly by fax, e-mail or post or by any other means including those listed in PETRONAS' privacy statement. You should therefore monitor any relevant sources on a daily basis.

7.2. Practical steps must be taken when you receive a request for information includes:

(a) Whether or not there is a legal basis for the request, we should always acknowledge the request as soon as possible.

(b) The LCD, of Group Legal team should then be informed so that they can make an assessment of whether it is legitimate (i.e. not manifestly unfounded or excessive) and how the request should be properly responded to. All requests should be alerted to the LCD, of Group Legal as some jurisdictions impose strict deadlines for response and we may be sanctioned if we do not adhere to such deadlines.

(c) When you receive a request from a data subject, you should immediately contact the LCD, of Group Legal. You should do this promptly as it generally takes some time to identify which information we hold about a data subject across all the databases we maintain. You may not be able to respond in time if you delay this request.

(d) It is important to remember that you may only provide personal information about the data subject who is making the request. You should make sure that you have properly identified the correct data subject. It is important to make sure that we can confirm the identity of the individual who has made the request, before we provide any information. Please ask them a number of control questions to verify their identity (e.g. mother's maiden name, postcode, date of birth). If we don't not hold such information or you are unsure how to verify the data subject's identity, please contact the LCD, of Group Legal.

(e) If you receive a request for restriction, you should get in touch with the LCD, of Group Legal as soon as possible and 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, personal data can only be processed with the data subject's consent or in relation to a legal claim.

Guideline 8. Complaint handling

8.1. If a data subject feels that we are processing their personal data improperly or where we have failed to respond effectively to their request to exercise their rights, he/she may make a complaint. It is likely that in the first instance the complaint will be made to us directly. However, if we fail to address the complaint, the data subject may escalate the matter to the competent supervisory authority. The supervisory authority will then investigate the matter.

8.2. In the event that you receive such a complaint, you should immediately bring it to the attention of the LCD, of Group Legal and the Data Protection Officer (if applicable) to resolve the complaint.

8.3. Complaints received from data subjects or supervisory authorities should be treated seriously and dealt with efficiently. We should always acknowledge receipt of a complaint and provide information about the timing of a full response. To the extent prescribed by a supervisory authority, we should stick to any deadlines communicated to us. The exact procedure for responding to a request or complaint from a supervisory authority will depend on the context and subject matter of the issue. Always inform the LCD, of Group Legal and/or Data Protection Officer (if applicable) if you receive a communication from a supervisory authority.

SECTION 5 - USE OF THIRD PARTY SUPPLIERS/PROCESSORS

Guideline 9. Differences between a Data Controller and a Data Processor

9.1. When handling personal data it is important to understand the difference between a data controller and a data processor. This is because many personal data protection and privacy laws make a distinction between the two, with most of the legal obligations is upon the data controller to ensure the personal data is adequately protected.

(a) The data controller (please refer to the Glossary) is the person who will generally be held primarily liable for any breaches of personal data protection and privacy law because they have control of a data subjects' personal data and can decide what the data is used for and where it is kept.

(b) In contrast, a data processor (please refer to the Glossary) is generally only responsible for performing the tasks given to them by the data controller. Processing carried out by a processor will usually (and under some data protection laws, must be) be governed by a contract and it is the contract that will set out the responsibilities of the parties towards each other.

(c) The contract between a data processor and a data controller should also seek to deal with any liability issues vis-a-vis the two parties. Please contact the LCD, of Group Legal if you require assistance in connection with contracts to be entered into with data processor and a data controller.

Guideline 10. Our responsibility

10.1. In our everyday operations we rely on third parties to provide us with services to support our business. These services include a number of personal data handling activities, such as sending and receiving e-mails, invoicing, payroll processing, marketing database management, etc. To provide these services, we will need to transfer personal data outside the organisation to people who will be processing the data on our behalf. These people/companies are, data processors.

10.2. We need to ensure that our data processors take all reasonable precautions to maintain the security of the data and, in particular:

(a) To prevent the personal data being altered or damaged or accessed by people who are not unauthorized to look at it.

(b) When we transfer the personal data to third party data processors, we remain legally responsible for that personal data even though we may no longer have direct control. For that reason, we must ask data processors to provide us with adequate guarantees to ensure the implementation of security and confidentiality. These guarantees should be included in the contract which we sign with the third party.

10.3. Please contact the LCD, of Group Legal if you require assistance in connection with contracts to be entered into with data processors.

Guideline 11. Responsibility for our service providers

11.1. We are responsible for the security and integrity of the information we gather on data subjects. So whenever we send information to service providers (for example, to payroll or marketing outsourcing service providers), we must ensure that these service providers treat the information with at least as much care as we do.

SECTION 6 – EXPORTING OF PERSONAL DATA

Guideline 12. Personal Data Transfer Obligations

12.1. In the course of our business it is likely that we will need to send personal data about, for example, employees or customers, to a third party or another PETRONAS group of companies or a third party service provider located in another jurisdiction. When doing this, you need to be aware that there are restrictions to such transfers exist under various personal data protection and privacy laws. The rules are different depending on the location of export.

12.2. Transfers between PETRONAS group companies are governed by a set of contractual clauses which ensure the security of the data transferred. When personal data is exported to entities outside of the PETRONAS group of companies, the LCD, of Group Legal will need to be informed to ensure that any such transfer is made in compliance with applicable laws governing data transfers and data localisation.

12.3. It may be that if you send personal data to another country, the recipient in that country will need to send it on to yet another country to process the personal data. It is therefore important that, before you proceed with any international transfer of personal data, you find out whether such personal data will be transferred again and, if so, where to.

SECTION 7 - MARKETING

Sending marketing and public relations material to our clients and customers is part of our business. However, large/unfocused marketing campaigns can also generate a lot of complaints from people who do not wish to hear from us. A failure to address these concerns proactively can be a source of risk for our business. For that reason, we should take a number of simple precautions as set out below.

Guideline 13. Direct vs. Indirect marketing

13.1. Direct marketing means any advertising or marketing communication that is directed at particular individuals (or, in some jurisdictions, companies).

13.2. Indirect marketing means any marketing targeted at a general audience (e.g. billboards, television, trade magazines adverts etc.).

13.3. Unlike indirect marketing, direct marketing requires us to collect and use personal data. Accordingly, the personal data protection and privacy rules provide for certain safeguards to the benefit of customers and other people to whom we directly market products. These safeguards are designed to ensure that these people have agreed to us sending them marketing materials or, at least, have the right to object to future use of their personal data for direct marketing purposes where we send them marketing information that they have not requested (this is referred to as unsolicited marketing). These rules can apply to telephone (including voicemail messages and automated calls), fax, e-mail and SMS marketing.

Guideline 14. General principles – Opt-in or Opt-out on Marketing Matters

14.1. As with any processing of personal data (including collection of this personal data), we must tell people what we are using their personal data for. We can do this in a number of ways such as:

(a) including specific information in the marketing materials we send out,

(b) when collecting material on-line, using pop-ups or links which provide further information, and

(c) by referring to our on-line privacy statement.

14.2. It is good practice to make sure that our privacy statement is broad enough to cover the activities mentioned in a particular direct marketing campaign before we launch it. If it is not broad enough we can still use the personal data provided we are clear in our marketing material what we intend to do with the information.

14.3. The rules for direct marketing products and/or services to customers or other recipients generally depend on the method through which we propose to contact these people. Some countries also maintain databases with which people can register to avoid being contacted by post, telephone or fax.

Opt-in (affirmative consent) and Opt-out (right to object) on marketing matters

14.4. Depending on the jurisdiction, the e-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 the LCD, of Group Legal to determine whether it is necessary to launch campaigns to collect consent of contacts in certain countries prior to sending them direct marketing material.

14.5. Regardless of whether such "opt-in" is required, remember that we must always provide a simple way of "opting out" on all direct marketing communications we send out, whether by fax, mail, e-mail or SMS (for example, a link towards an opt-out page or a number to which a data subject may send a text message).

14.6. If a data subject opts out of unsolicited marketing communications, we must ensure that we record this in the database entry that relates to this data subject. Simply deleting the personal data is not sufficient and may create problems as we must record the data subject's choice for the future, even if we obtain that data subject's contact details again through another source.

14.7. If a data subject has opted out, we must refrain from sending unsolicited direct marketing material to him/her.

14.8. The data subject's right to object should be brought to its attention, at the latest, when the first direct marketing communication is made. The data subject's right to object must be presented to them clearly and separately from any other information.

SECTION 8 - OTHER PERSONAL DATA PROTECTION REQUIREMENTS

Guideline 15. Appointment of a Data Protection Officer

15.1. In certain jurisdictions, where:

(a) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale;

(b) the core activities of the controller or the processor consist of processing sensitive data, or personal data relating to criminal convictions and offences, on a large scale, or

(c) you are a public authority or body,

it is mandatory to appoint a Data Protection Officer.

15.2. Even where not mandatory, or where the type of processing does not give rise to the mandatory requirement, Data Protection Officers can be appointed in order to monitor and ensure compliance with personal data protection and privacy laws.

Guideline 16. Training of staff

16.1. There may be training sessions on personal data protection matters during the year, which you should attend. You should also follow the mandatory on-line training when requested to do so.

16.2. Besides attending these training sessions, it is your responsibility to refer to these Guidelines when you are dealing with personal data. In case of doubt, you may contact the LCD, of Group Legal with questions on the application of these Guidelines.

GLOSSARY

The following sets out key terms and concepts used when dealing with personal data protection issues. Please note that terminology differs depending on the jurisdictions, but the concepts will often be the same or similar.

Consent. Consent of the data subject means that the data subject has given an indication that they agree to the processing of his/her personal data. 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. Please see Guideline 2 for further information regarding "*specific, informed and unambiguous*" indications of consent.

Data controller. A data controller is the person (individual, company or public body) which, alone or jointly with others, determines the purposes and means of the processing of personal data. A single processing of personal data may have multiple controllers.

Data processor. A data processor is the person (individual, company) who processes personal data on behalf of the data controller (but does not determine the purpose or means of such processing). This may be an affiliate of the data controller or a third-party providing outsourcing services.

Data subjects. The persons entitled to the protection of their personal data are called "data subjects". Data subjects are the identified or identifiable persons, whose data is being processed. An "identifiable person" is a person who can be identified, directly or indirectly, in particular by reference to an identifier, such as their name, an identification number, location data, an online identifier, or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

Personal data relating to criminal offences. Personal data relating to criminal convictions are considered very highly sensitive personal data, and may generally only be processed under the control of an official authority.

PETRONAS. The term "PETRONAS" means PETROLIAM NASIONAL BERHAD (PETRONAS) and its subsidiaries and controlled companies. The expression "PETRONAS" is used for convenience where references are made to PETRONAS group of companies in general. The companies in which PETROLIAM NASIONAL BERHAD (PETRONAS) has direct or indirect shareholding are distinct legal entities.

Processing. Processing means the operation or set of operations which are performed on personal data, whether or not by automatic means, such as the collection, organization, storage, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction (i.e. marking data for limited uses only), erasure or destruction.

Restriction. Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future.

Special categories of data or "sensitive personal data". Generally, personal data revealing racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, data concerning health or sex life, genetic data, commission or alleged commission of any offence, and biometric data for the purpose of uniquely identifying a natural person are considered especially sensitive personal data, and their collection and processing are subject to specific rules.

Supervisory authority. Supervisory authority means an independent public authority which is established to monitor the application of, and compliance with, data protection law.

APPENDIX A

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 the Master 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. the Master 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 the law as at the version date of this checklist and has not been updated unless otherwise indicated. You must therefore check 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 Legal Compliance Department (LCD) of Group Legal.

PERSONAL DATA PROTECTION PRINCIPLE	CHECKLIST ITEMS	REMARKS
COLLECTION OF PERSONAL DATA		
Collection of Data (consider both manual and electronic data)	Collection of personal data adequate (and not excessive) Sample: HR collects data fields as follows: ▪ Name ▪ Age ▪ Address ▪ Religion ▪ Name of Parents ▪ Political Affiliation	
	Collection of minors' personal data – If yes, whether consent of parent / guardian obtained?	
	Privacy by Design / by Default ▪ Has personal data protection and privacy been considered at the commencement/ of operations?	

PERSONAL DATA PROTECTION PRINCIPLE	CHECKLIST ITEMS	REMARKS
	▪ Has there been appropriate measures to ensure only necessary personal data collected? ▪ Is personal data collected accurate? ▪ Should data fields by anonymized / pseudonymized?	
Consent Principle	Obtaining Consent – Customers Sample: For customers, consent is obtained via service agreement. *[or to state if any exemption under the law applies:* ▪ *Contractual Necessity* ▪ *Legal Obligation* ▪ *Vital Interests* ▪ *Public Interests* ▪ *Legitimate Interests]*	
	Obtaining Consent - Employees	*[or to state if any exemption under the law applies]*
	Obtaining Consent – Vendors, Suppliers, etc	*[or to state if any exemption under the law applies]*
	Records of consent – Customers	
	Records of consent – Employees	
	Records of consent – Vendors, Suppliers, Third Party Service Providers*	
Accuracy Principle	Practical steps to ensure accuracy of personal data collected For example: Send regular emails to employee to request for any updates (i.e. GHRM through Mypassport)	
	Additional security requirements? (based on local applicable laws)	

PERSONAL DATA PROTECTION PRINCIPLE	CHECKLIST ITEMS	REMARKS
Notice Principle	Privacy Notice for Customers	
	Privacy Notice for Employees	
	Privacy Notice for Vendors, Suppliers, Third Party Service Providers	
	CCTV Notice	
	Has Privacy Notice been communicated to the data subjects?	
	Multi-lingual*	
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)	

PERSONAL DATA PROTECTION PRINCIPLE	CHECKLIST ITEMS	REMARKS
	▪ Regularly monitor compliance within organisation and also outside (third parties)	
	Additional security requirements? (based on local applicable laws) • Keep in a secured filing room- insert PDPA standards.	
Accuracy Principle	Practical steps to ensure accuracy of personal data maintained and kept (e.g. regular check)	
	Additional security requirements? (based on local applicable laws)	
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 there disposal schedule maintained?	
	Additional retention requirements? (based on local applicable laws)	
HANDLING ENQUIRIES AND REQUESTS ON PERSONAL DATA		
Access and Correction Principle	Is there data access/ data correction procedure?	
	Is there method for data subjects to access and correct personal data (e.g. online portal)	
	Period for compliance with data access/ data correction	
OUTSOURCING DATA PROCESSING OPERATIONS/DATA PROCESSORS		
Data Processors	Are there data processors? If yes, see below.	
	Are there contracts entered with the data processors?	
	Are there sufficient security obligations imposed on data processors?	

PERSONAL DATA PROTECTION PRINCIPLE	CHECKLIST ITEMS	REMARKS
	Are there sufficient guarantees obtained from the data processors as to security of personal data?	
EXPORTING DATA		
Transfer of Personal Data Abroad	Are there transfer of personal data outside the jurisdiction? If yes, see below.	
	Consent of data subjects	*[or to state if any exemption under the law applies]*
DIRECT MARKETING		
Direct Marketing	Is there direct marketing activities? If yes, see below.	
	Has consent been obtained from data subjects for marketing activities?	
	Is there opt-out option provided to the data subjects?	
	Do-Not-Call / No-Marketing Registry	
OTHER DATA PROTECTION REQUIREMENTS (WHERE APPLICABLE)		
Registration as Data Users*	PDPA certificate of registration (where applicable) *	
	Display of certificate in the premises*	
Miscellaneous	Data Protection Officer (where applicable)	
	Regular training of staff on personal data protection and privacy compliance	
	Compliance Manual	
	Website Cookie Policy	

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