PERSONAL DATA PROTECTION CODE OF PRACTICE

FOR THE MALAYSIA AVIATION SECTOR

21 NOVEMBER 2017

THE PERSONAL DATA PROTECTION CODE OF PRACTICE

For the Transportation Sector (Aviation)

21 November 2017

PESURUHJAYA PERLINDUNGAN DATA PERIBADI

Ref. No.
CoP_AVN

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

Dated: 21 November 2017 .

(KHALIDAH BINTI MOHD DARUS)
Personal Data Protection Commissioner, Malaysia

TABLE OF CONTENTS

1.0 Introduction to the PDPA and COP

1.1 The PDPA sets out seven data protection principles, which are the:

(a) General Principle
(b) Notice and Choice Principle
(c) Disclosure Principle
(d) Security Principle
(e) Retention Principle
(f) Data Integrity Principle
(g) Access Principle

1.2 Breaches of the PDPA attract criminal liability. The fines range between RM 10,000 and RM 500,000. Terms of imprisonment of up to a maximum of three (3) years may be imposed. There is also personal liability for directors, chief executive officers, chief operating officers, managers, secretaries and other similar officers unless he / she can establish that: (1) the offence was committed without his / her knowledge; and (2) he / she had taken all reasonable precautions and exercised due diligence to prevent the commission of the offence.

1.3 These PDPA principles set out obligations of Data Users in broad terms. However, the PDPA recognises that separate industries have different business practices. It grants each Data User the discretion and flexibility to address compliance by requiring a separate code of practice for each class of data users. The purpose, application and effect of this Code is elaborated further in Chapter 2.

1.4 This Code combines the requirements set out in the PDPA, Regulations and Standards to explain how these data protection laws apply to the handling of personal data by the aviation sector and provides good practice advice for the aviation sector. In this Code, certain words are used. These words are defined in **Appendix 1: Definitions / Glossary**.

Who does the Code apply to?

1.5 The Code applies to licensees and/or permit holders under the Malaysian Aviation Commission Act 2015, including:

(a) Malaysia Airlines Berhad;
(b) AirAsia Berhad;
(c) AirAsia X Berhad;

(d) MASwings Sdn. Bhd.;
(e) Malindo Airways Sdn Bhd;
(f) Berjaya Air Sdn Bhd; and
(g) FlyFirefly Sdn Bhd.

1.6 This Code applies to all Personal Data and/or Sensitive Personal Data handled by these Data Users in commercial transactions.

How the Code can help

1.7 Although the PDPA sets out the broad legal requirements to be followed when processing Personal Data, it does not provide guidance on practical measures that could be taken to comply with them. The Code helps to fill this gap.

1.8 This Code will help Data Users to identify the issues they need to consider when processing Personal Data. It will provide Data Users with confidence on the appropriate steps to take with regard to Personal Data and give a clearer idea of what is not acceptable when dealing with Personal Data. Specific benefits of this Code include:

(a) minimised risk of breaking the law and consequent enforcement action by the Commissioner;
(b) better public trust by ensuring that legally required safeguards are in place and complied with;
(c) better protection for Data Subjects when their data is processed;
(d) greater trust and a better relationship with the individuals whose Personal Data is being processed;
(e) reduced reputational risk caused by the inappropriate practices with regard to processing Personal Data;
(f) a better understanding of what and what is not acceptable when dealing with Personal Data; and
(g) reduced risk of questions. complaints and disputes about the manner in which Data Users handle Personal Data.

1.9 This Code has the force of law and is effective once it is registered by the Commissioner in the Register of Code of Practice ("**Effective Date**"). It is binding on Data Users, shall comply with the Code within a period to be determined and notified in writing by the Commissioner. As the Code is legally binding, Data Users who fail to comply with this Code are regarded as having committed

an offence, and upon conviction, are liable to a fine of up to RM 100,000 or to imprisonment for a term of not more than one (1) year or to both under Section 29 of the PDPA.

1.10 This Code shall complement the PDPA and any regulations, orders, standards, directions, guidance or other similar regulatory instrument issued pursuant to it.

1.11 In the event of a conflict between this Code and any standards set out by the regulators of the aviation industry as may be prescribed by law, the document setting the higher standard will prevail to the extent of any conflict.

1.12 The examples provided in this Code are not intended to be exhaustive but are included for context and for the purposes of illustration.

1.13 This Code is an interpretation by the aviation sector of what the PDPA requires when dealing with Personal Data. The recommendations provided in this Code are good practice and Data Users are encouraged to adopt these practices.

2.0 PDPA in Practice

(A) Background

What is Personal Data?

2.1 The aviation industry generates vast amounts of data ranging from engineering and scientific data to consumer data, passenger data and security data. However, not all data is Personal Data. This section of the Code provides guidance on what is or is not considered to be Personal Data.

2.2 The following data would be considered Personal Data:

(a) personally identifiable information such as name, gender, date of birth, nationality, passport/identification card number and country of residence;

(b) the details of a passenger's health condition, such as whether a passenger is expecting;

(c) the details of a passenger's payment information such as payment information contained in e-wallets, prepaid account information, credit or debit card information;

(d) the details of an individual's dietary preferences and in-flight spending patterns, when processed with personally identifiable information.

(e) the details of an individual's flight information including flight number and seat number, currency, departure destination; and

(f) the details of an individual's loyalty account number (if any).

2.3 The following data would not be considered as Personal Data:

(a) business contact information, as further discussed below;

(b) site traffic patterns;

(c) data relating to deceased individuals;

(d) data relating to individuals which has been aggregated and/or anonymized in such a manner as to render the individual non-identifiable; and

(e) electronically archived and / or backed-up data.

What is Business Contact Information?

2.4 Business contact information refers to information processed in a business-to-business context such as information of a company's officers, authorized signatories, directors, individual shareholders, individual guarantors, individual security providers, suppliers, vendors or key contact information. The PDPA does not expressly exempt business contact information. However, the Commissioner has taken the position that dealings with business contact information are low risk.

2.5 A Data User may obtain business contact information when dealing with an organization or company in the course of business. In such instances, the Data User is entitled to assume that the organization or company is authorized to provide the information to the Data User.

2.6 Data Users are not required to obtain the consent of these business contacts in order to process their information for the purposes of a business transaction between the Data User and the organization or company.

2.7 However, if the Data User uses the Personal Data of these business contacts for purposes unrelated to the business transaction, such as offering flight offers to the business contact in his or her personal capacity, such business contacts will then be considered as Data Subjects under the PDPA.

***Example A**: Airline X enters into negotiations with an in-flight caterer to provide new in-flight catering services. Airline X obtains information of the in-flight caterers' directors, authorized signatories, key contact persons and individual shareholder. Airline X is: (i) entitled to assume that the in-flight caterer is authorized to provide such information; and (ii) is not required to obtain the consent of the director, authorized signatory, key contact person or individual shareholder in order to process their information.*

What is Sensitive Personal Data?

2.8 Sensitive Personal Data includes the following:

(a) a passenger's physical condition such as whether the passenger is expecting;

(b) a passenger's physical health such as whether the passenger has been ill prior to boarding a plane or whether the passenger has a disability;

(c) a passenger's religious beliefs; and

(d) a passenger's prior criminal history (if any).

2.9 Data Users are required to obtain the **explicit** consent of the Data Subject prior to processing Sensitive Personal Data.

2.10 If the Data User is unable to obtain explicit consent or where it is not feasible or practicable for the Data User to do so, Sensitive Personal Data may be processed where the processing is necessary for:

Employment

(a) for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the Data User in connection with employment;

Vital Interests

(b) in order to protect the vital interests of the Data Subject or another person, in a case where:

(i) consent cannot be given by or on behalf of the Data Subject; or

(ii) the Data User cannot reasonably be expected to obtain the consent of the Data Subject.

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

Medical Purposes

(c) for medical purposes and is undertaken by:

(i) a health professional; or

(ii) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare professional;

Legal Proceedings

(d) for the purpose of, or in connection with legal proceedings;

Legal Advice

(e) for the purpose of obtaining legal advice;

Defending Legal Rights

(f) for the purpose of establishing, exercising or defending legal rights;

Administration of Justice

(g) for the administration of justice;

Lawful Functions

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

Public Information

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

What is Processing?

2.11 The PDPA applies to Personal Data and Sensitive Personal Data that is "processed". The term "processed" applies to a comprehensive range of activities and includes the initial collection of Personal Data, the retention and use of it, access, disclosure and final disposal.

2.12 **Appendix 2: Data Flow** sets out how personal data is usually collected and processed by airlines and how personal data should be managed according to the seven data protection principles.

2.13 The processing of Personal Data and Sensitive Personal Data is subject to the seven data protection principles as further discussed below.

(B) General Principle (Section 6 of the PDPA)

What is the General Principle?

2.14 The General Principle provides:

(a) Data Users are required to obtain consent prior to processing Personal Data. However, consent need not be obtained in all instances.

(b) explicit consent is required to process Sensitive Personal Data. This is further discussed below;

(c) the collection and processing of Personal Data must be adequate, relevant and not excessive to the purpose for which Personal Data is collected and processed.

2.15 Consent is not required where processing of Personal Data is:

(a) requested by the Data Subject with a view to enter into a contract;

Example: *Where a potential passenger wishes to book a flight from the Data User, he must enter into a contract with the Data User, which is the Data User's carriage agreement. Consent is not required to collect the passenger's name and contact information for the purpose of the entering into a contract with the Data User.*

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

Example: *Where a passenger has booked a ticket and entered into a carriage agreement with the Data User, consent is not required for staff of the Data User to request for the passenger's name and passport number for the purposes of verifying the passenger's identity and checking the passenger into the flight.*

(c) to comply with any legal obligation of the Data User, other than an obligation imposed by a contract;

Example: *Where the Data User is required to provide Personal Data of its passengers to by a committee established under the Malaysian Aviation Commission Act 2015 to investigate a consumer complaint against the Data User.*

(d) to protect the vital interests of the Data Subject;

Example: *Where the Data User discloses names and nationalities in search and rescue operations in the event of an aircraft incident.*

(e) for the administration of justice; or

Example: *Where a Data User is obligated to disclose Personal Data to an officer authorized under any written law for the purpose of investigations or prosecution.*

(f) for the exercise of any functions conferred upon on any person under any law or if an order from a court of law requires the disclosure of the Personal Data.

Example: *Where an airline receives a court order to disclose details of passengers which boarded a particular flight pursuant to prosecution proceedings where the whereabouts of those passengers are relevant to establishing the prosecutor's case.*

How to Obtain Consent?

2.16 Consent should be obtained before personal data is collected. For airlines, personal data is usually collected at the following collection points:

(a) ticket counters;
(b) call centres;
(c) travel agents;
(d) online, through websites or mobile applications; and
(e) through e-mails or letters (for chartered flights and group bookings)).

2.17 If Sensitive Personal Data is collected, explicit consent must be obtained through a various channel predetermined by the standard operation procedures of data user.

2.18 Where Sensitive Personal Data is collected through other channels, such as in person, via recording explicit consent or via an online personal data collection form for various purposes such as where passenger requests wheelchair services, selection of seats in the emergency row due to a particular health condition or where the passenger is expecting, the Data Subject must be required to expressly indicate his / her consent. For example, the Data Subject may be required to provide his / her signature to indicate consent or to check an appropriate consent box.

Ticket Counters

2.19 Personal data is collected when a customer provides his / her name, identification number and other contact details when purchasing flight tickets through airport ticket counters or ticket counters in rural areas.

2.20 Strictly speaking, consent is not required to process personal data where the processing is requested by the Data Subject with a view to enter into a contract. The contract in this case is the contract of carriage between the airline and the Data Subject. However, if Sensitive Personal Data is obtained (such as whether the passenger has a specific health condition or is expecting), written explicit consent must be obtained by requiring the Data Subject to either provide his / her signature indicating consent or to check the appropriate consent box.

Call Centres

2.21 Personal data is collected when a customer provides his / her name, identification number and other contact details when purchasing flight tickets over the phone at the airline's call centre.

2.22 Strictly speaking, consent is not required to process personal data where the processing is requested by the Data Subject with a view to enter into a contract. The contract in this case is the contract of carriage between the airline and the Data Subject. However, if Sensitive Personal Data is obtained (such as whether the passenger has a specific health condition or is expecting), verbal explicit consent must be obtained from the Data Subject.

Check-In Counter

2.23 Personal data is collected when a customer provides his / her name, identification number and / or passport number during check-in at the airport check-in counter.

2.24 Strictly speaking, consent is not required to process personal data where the processing is requested by the Data Subject with a view to enter into a contract. The contract in this case is the contract of carriage between the airline and the Data Subject. However, if Sensitive Personal Data is obtained (such as whether the passenger has a specific health condition or is expecting), written explicit consent must be obtained by requiring the Data Subject to either provide his / her signature indicating consent or to check the appropriate consent box.

2.25 However, the airline must still provide the Privacy Notice to the customer**.** It is recommended that the airline displays the Privacy Notice at a prominent place at the ticket counter and provide a hard copy of the Privacy Notice upon request.

Travel Agents

2.26 Personal data of passengers such as names and contact details may be disclosed by travel agents to the airline. Sensitive Personal Data of the passengers such as the passengers' health condition may also be disclosed by travel agents.

2.27 In this instance, the airline should obtain the appropriate warranties from the travel agents that the travel agents have complied with the PDPA in obtaining the Personal Data and Sensitive Personal Data of customers.

2.28 Airlines may use the sample clauses provided in **Appendix 5: Personal Data Disclosed or Received From Third Parties.**

Online Collection

2.29 Personal data may be collected from the customer when the customer creates a member account with the airline's website. The customer may be prompted for his / her name, e-mail address and hand phone number when creating an online account.

2.30 Strictly speaking, consent is not required to process personal data where the processing is requested by the Data Subject with a view to enter into a contract. The contract in this case is the contract of carriage between the airline and the Data Subject if the personal data is collected solely for the purposes of enabling the purchase of flight tickets.

2.31 However, the airline may wish to also send the customer updates and offers or ask the customer to join a loyalty program. In such a case, the airline must obtain the consent of the customer. **Appendix 3: General Principle** provides a template form of consent for online collection of Personal Data. Further, if Sensitive Personal Data is provided by the customer, written explicit consent must be obtained by requiring the Data Subject to either provide his / her signature indicating consent or to check the appropriate consent box.

2.32 Where the Data Subject books tickets on behalf of friends or family members and provides Personal Data of friends and family members (which may sometimes be children) to the airline. The airline should ensure that the customer who provides the warranty is above eighteen (18) years of age and has the appropriate authority and consent of third parties whose Personal Data is submitted to the Data User.

In Practice

2.33 The airline should identify which Personal Data collection points are relevant to its operations and ensure that the appropriate consent language and mechanisms are in place at these collection points.

(C) Notice and Choice Principle (Section 7 of the PDPA)

2.34 The Notice and Choice Principle provides that Data Users must make a written notice available to Data Subjects before or as soon as possible after collecting and processing Personal Data. This written statement is also known as a Privacy Notice.

2.35 The Privacy Notice is a publicly available statement which clearly sets out the privacy practices of a Data User.

2.36 **Appendix 4: Notice and Choice Principle** sets out a template Privacy Notice which may be used by the Data User.

How may the Privacy Notice be communicated?

2.37 The Privacy Notice should be communicated at all the points where Personal Data is collected. These are:

Ticket Counters

2.38 It is recommended that the airline displays the Privacy Notice at a prominent place at the ticket counter and provide a hard copy of the Privacy Notice upon request.

Call Centres

2.39 It is recommended that a hyper link to the Privacy Notice be incorporated on the flight ticket which is subsequently issued to the customer

Check-In Counter

2.40 It is recommended that the airline displays the Privacy Notice at a prominent place at the ticket counter and provide a hard copy of the Privacy Notice upon request.

Travel Agents

2.41 Personal data of passengers such as names and contact details may be disclosed by travel agents to the airline. Sensitive Personal Data of the passengers such as the passengers' health condition may also be disclosed by travel agents.

2.42 In this instance, the airline should obtain the appropriate warranties from the travel agents that the travel agents have complied with the PDPA in obtaining the Personal Data and Sensitive Personal Data of customers including providing customers with the appropriate Privacy Notice.

2.43 Airlines may use the sample clauses provided in **Appendix 5: Personal Data Disclosed or Received From Third Parties.**

Online Collection

2.44 The Privacy Notice may be provided to the client prior to opening an online account or prior to the online purchase of flight tickets by the client.

2.45 Where Personal Data was collected prior to the enforcement of the PDPA, the Data User is required to provide Data Subjects with a Privacy Notice prior to:

(a) using the Personal Data for purposes other than the original purpose for which it was collected; and

(b) disclosing the Personal Data to any Third Party.

Example: *The Data User may send e-mails to the Data Subjects informing them of the updated Privacy Notice or make an announcement at the Data User's corporate website or corporate mobile app of the Data User's updated Privacy Notice.*

2.46 The Data User may also communicate their Privacy Notice, and it is deemed to be communicated, to the Data Subject by using one or more of these methods:-

(a) by posting a printed copy of the Privacy Notice to the last known address of the Data Subject; or

(b) by posting the Privacy Notice on the corporate website of the Data User; or

(c) by informing the Data Subject through instant messaging containing a corporate website address/link to the Privacy Notice and/or a telephone number to request for further information; or

(d) by inserting a summary of the Privacy Notice in regular communications with the Data Subject with a corporate website address/link to the Privacy Notice and/or telephone number if the Data Subject wishes to request for further information; or

(e) by prominently displaying a summary of the Privacy Notice at the Data User's place of business and making available the full Privacy Notice upon request at the Data User's counter; or

(f) by displaying a message on the screens of a Data User's self check-in kiosk with a corporate website address/link to the Privacy Notice, a telephone number to request for further information and/or stating that the Privacy Notice is available at the Data User's branch office; or

(g) by inserting a statement in application / registration forms referring to the Privacy Notice, and providing a link to the corporate website, or a telephone number to request for further information; or

(h) by printing out copies of the Privacy Notice and providing it to the Data Subject at the Data User's premises; or

(i) any other method of communicating the Privacy Notice as approved by the Commissioner or that brings the Privacy Notice to the attention of the Data User.

Example: *Where the Data User provides a summary of the Privacy Notice together with a link to the Privacy Notice in its corporate website in its e-mail communications with the Data Subject, this is sufficient to prove that the Privacy Notice has been communicated to the Data Subject.*

2.47 The Data User should determine the most appropriate method of communicating the Privacy Notice which would reach as many of its Data Subjects as possible. It is recommended that Data Users uses a variety of methods of communication to ensure that the Privacy Notice is communicated as widely as possible.

Example: *Some Data Subjects may not be computer literate. In this instance, the airline may communicate the Privacy Notice over the telephone when a ticket booking is made or by displaying a summary of the Privacy Notice at walk-in ticket booking counters and making a copy of the Privacy Notice available on request.*

2.48 The Privacy Notice, when communicated by Data User to the Data Subject, shall be deemed to have been communicated on behalf of the Data User's subsidiaries, holding, associates and related companies.

2.49 It is permissible for the Privacy Notice to be issued by the holding company where the Data User is a subsidiary within a larger group of companies.

2.50 It is recommended that Data Users communicate the Privacy Notice to all Data Subjects, whether existing or new, as this will minimize the Data User's administrative burden in ensuring compliance.

When is the Privacy Notice Accepted?

2.51 The PDPA does not require proof that the Privacy Notice is received and/or accepted by the Data Subject.

2.52 The Privacy Notice will be deemed to have been communicated to the Data Subject each time the Data Subject uses the Data User's services / facilities and is provided with Privacy Notice through the methods of communication set out above.

Keeping Records

2.53 Data Users are required to maintain records of having communicated the Privacy Notice to Data Subjects. This requirement may be fulfilled where the Data User maintains evidence / records that the Privacy Notice has been communicated to the Data Subject.

Example: *Where the Privacy Notice is communicated to Data Subjects by prominently displaying a summarised version of the Privacy Notice at the Data User's place of business and making a full Privacy Notice available at the counter, the production of the summarized Privacy Notice and the full Privacy Notice shall be sufficient to prove that the Privacy Notice has been communicated to Data Subjects.*

Example: *Where the Privacy Notice is communicated by e-mail to Data Subjects, the production of the e-mail referring to the Privacy Notice, the Privacy Notice itself and the provision of names of Data Subjects that the e-mail was sent to, shall be sufficient to prove that the Privacy Notice has been communicated to Data Subjects.*

Example: *Where the Privacy Notice is communicated by SMS to Data Subjects, the production of the text of the SMS referring to the Privacy Notice, the Privacy Notice itself, and the process for communicating the SMS to Data Subjects, shall be sufficient to prove that the Privacy Notice has been communicated to Data Subjects.*

In Practice

2.54 It is recommended that the Data User identifies its Personal Data collection points and ensure that the mechanisms for making Data Subjects aware of its Privacy Notice is in place at these collection points.

(D) Disclosure Principle (Section 8 of the PDPA)

2.55 "Disclosure" is not defined in the PDPA. A Data User can be taken to have "disclosed" Personal Data when it makes Personal Data available to a Third Party.

2.56 The purpose declared by the Data User for the collection of Personal Data in the Privacy Notice is of importance as it affects whether additional consent needs to be obtained under the Disclosure Principle. The Disclosure Principle is closely related to the Notice and Choice Principle.

2.57 A Data User may only disclose Personal Data:

(a) in accordance with the Privacy Notice;

(b) in accordance with all statutory or contractual requirements; or

(c) for purposes authorised by the Data Subject.

What Disclosures are Permitted?

Permitted Disclosures based on the Privacy Notice

2.58 The Disclosure Principle provides that the Data User may disclose Personal Data to Third Parties where:

(a) the disclosure is for a purpose declared at the at the point of collection as stated in the Privacy Notice; or

Example: *The Data User may have informed the Data Subject that Personal Data may be disclosed to authorised third party service providers in the Privacy Notice for the purposes of enabling certain business functions to be carried out such as sharing of Personal Data with IT service providers for IT maintenance services.*

(b) the disclosure is for a purpose directly related to the purpose declared in the Privacy Notice at the point of collection; or

Example: *Where a Data User has informed the Data Subject that Personal Data may be disclosed to IT service providers for IT maintenance services, an example of a directly related purpose would be disclosures to various personnel of the IT service provider for various IT maintenance purposes.*

(c) the disclosure is being made to a Third Party mentioned in the Privacy Notice or to a class or category of Third Parties as identified in the Privacy Notice (while still complying with applicable laws, regulations, standards and guidelines).

Example: *Where the Data User has informed the Data Subject that Personal Data may be disclosed to partner airlines for the purposes of facilitating flights. The relevant category of Third Party in this case would be the partner airlines.*

Permitted Disclosures under the law

2.59 Personal Data may be disclosed for any purpose or to any person not mentioned in the Privacy Notice under the following circumstances:

(a) <u>Consent</u>

The Data Subject has given his/her consent to the Disclosure;

(b) Crime

To prevent or detect a crime, or for investigations;

Example: *Where a fraud has been committed on the Data User and the Data User proceeds to disclose the information to a forensics specialist for internal investigation.*

(c) Law/ Court

Authorized by any law or court order;

Example*: Where the Data User is required to disclose information on passengers and flight information pursuant to a court order for disclosure.*

(d) Regulatory

To discharge regulatory functions;

(e) Legal Right

The Data User reasonably believed that it had in law the right to disclose the Personal Data;

Example: *Where the Data User is required to provide Personal Data of its passengers by a committee established under the Malaysian Aviation Commission Act 2015 to investigate a consumer complaint against the Data User.*

(f) Reasonable Belief

The Data User reasonably believed that the Data Subject will consent;

Example: *Where the Data User discloses Personal Data to the Data Subject's next of kin in the event of an emergency.*

(g) Public Interest

The Disclosure was made in the public interest as determined by the Minister;

(h) Tax

It is for the assessment or collection of any tax or duty or any other imposition of a similar nature;

(i) Statistics

It is for statistics or research in aggregated form with anonymised results and not used for anything else; or

Example: *Where the Data User conducts data analytics to analyse customer purchasing behaviour, provided that the resulting statistics are anonymized.*

Dealing with Requests for Disclosure

2.60 Where Personal Data is disclosed for the prevention or detection of crime or for investigation, the PDPA exempts Data Users from providing the Data Subject with information relating to the disclosure, even where a Data Access Request is filed by the Data User.

2.61 In dealing with requests for disclosures, Data Users will need to determine whether:

(a) the intended disclosure is permitted in accordance with the Privacy Notice; or

(b) the intended disclosure is exempted under the PDPA.

2.62 It is recommended that Data Users develop a disclosure policy which details the various instances where disclosure is permitted and the procedures to be followed when dealing with third party requests for disclosure.

2.63 If a request for disclosure is directed to a Data User by any regulatory or statutory authority, or where the disclosure is required or authorised by or under any law or by an order of court, the Data User must:-

(a) release the requested Personal Data upon receipt of written request citing the relevant legal basis of the request; and

(b) wherever appropriate, set conditions in relation to the permitted use of Personal Data and its return.

2.64 The Data User is not obliged to certify or verify Personal Data released, unless it is required by a court order.

Dealing with Disclosures to Data Processors

2.65 Data Users are likely to disclose Personal Data to Data Processors for various purposes relating to the Data User's business. For example, a Data User may engage an IT services provider to maintain its IT hardware and/or software systems. The Data User may also engage a data analytics and/or marketing agency to assist the Data User in identifying opportunities for marketing products to the Data User's customers.

2.66 Where Data Processors are engaged, it is recommended that the Data User obtains warranties from the Data Processor in respect of the Personal Data to be disclosed. These warranties may include, among others:

(a) that the Data Processor will only process Personal Data for purposes relating to its appointment by the Data User, in accordance with the Data User's instructions, and no other purpose; and

(b) the Data Processor will comply with all applicable laws, regulations and industry standards relating to the privacy, confidentiality or security of the Personal Data.

2.67 **Appendix 5: Personal Data Disclosed or Received From Third Parties** sets out some example clauses which the Data User may include in its agreement with Data Processors where Personal Data is disclosed to the Data Processor.

Keeping Records

2.68 The Regulations require a Data User to maintain a list of disclosures to Third Parties including Data Processors where these Third Parties are not included in the Privacy Notice.

2.69 A sample List of Disclosures is set out in **Appendix 5: Personal Data Disclosed or Received From Third Parties.**

In Practice

2.70 Where a Data User is able to foresee that disclosure of Personal Data to a certain class of Third Party may be required (whether as a matter of routine or due to the nature of the airline business), these Third Parties should be identified or mentioned in the Privacy Notice. To the extent that the Third Parties are not included in the Privacy Notice and the Data User wishes to disclose Personal Data to these Third Parties, the Data User should:

(a) obtain the consent of the Data Subject; and

(b) record the disclosure to this particular class of Third Party.

(E) Security Principle (Section 9 of the PDPA)

2.71 The Security Principle requires Data Users to keep Personal Data secure. Data Users are required to take practical steps to protect Personal Data from any "loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction."

2.72 The meaning of "practical steps" will vary from case to case, depending on the nature of Personal Data being processed by the Data User and the degree of sensitivity attached to the Personal Data or the harm that the Data Subject might suffer due to its loss, misuse, modification, unauthorized or accidental access, disclosure, alteration or destruction.

2.73 The Data User should take practical steps in implementing security measures to protect Personal Data within the control of the Data User, by taking into consideration the following:-

(a) the nature of Personal Data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access, disclosure, alteration or destruction;

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

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

(d) the measures taken for ensuring the reliability, integrity and competence of personnel having access to Personal Data; and

(e) the measures taken for ensuring the secure transfer of Personal Data.

Example: *If the Data User has employees who work from home, appropriate encryption measures and documents handling protocols should be put in place to ensure that it does not compromise security.*

2.74 The Data User shall assess their existing policies and implement measures, including but not limited to the following:

<u>Administrative</u>

(a) Confidentiality / Non-Disclosure Agreements;

(b) Supervision / monitoring of employees;

(c) Training and education plans for employees;

(d) Keep a record of employees who process Personal Data'

(e) Set authorisation limits for each Personal Data processing activity. Access to various Personal Data should be restricted to authorised employees by means of a user name and password;

(f) Revoke an employee's access rights to Personal Data when the employee no longer manages Personal Data or no longer works for the organization. For electronic means, the employee's user name and password should be cancelled;

Physical Security

(g) Door access system to control entry into and exit from premises where Personal Data is stored;

(h) store the personal data in a suitable location which is safe from physical or natural threats and is not exposed.

(i) provide close circuit security cameras (if necessary),

(j) provide 24 hour security control (if necessary);

(k) for Personal Data processed manually, the measures include:-

(i) ensure that Personal Data are stored in files in an orderly manner;

(ii) ensure that all files that contain Personal Data are stored in a locked place;

(iii) ensure that all keys are kept in a safe place;

(iv) maintain a record of where keys are kept; and

(v) store Personal Data in an appropriate location, where the Personal Data is safe from physical and natural threats and is not exposed.

Example: *As part of its security practices, the airline ensures that information on laptops and portable mobile devices issued to employees is encrypted. There is a protocol for dealing with stolen devices including immediately notifying IT services and enabling remote wipe-outs of information.*

Computer screens in the office are positioned so that they cannot be viewed by casual visitors. There is a system for paper disposal where paper waste is collected in secure bins and shredded on-site at the end of each week.

Technical Security

(l) encryption;

(m) anti-virus software.

(n) essential IT policies such as not opening e-mail attachments from unexpected or unknown sources;

(o) firewalls;

(p) software patching. Software patches are the latest updates from the creator of the operating system software or application software which usually contain fixes to potential security concerns;

(q) strict protocols regarding remote access (i.e employees' ability to access the network from a remote location). Access should be limited to specific IP addresses;

(r) ensuring that adequate security is in place where employees access company servers through a wireless network. The Data User should ensure that appropriate encryption measures, firewall, and secure web sessions are in place to protect against third party machine attacks when using unsecured wireless networks;

(s) portable laptops, USB keys, smart phones and other forms of portable devices should be encrypted and remote memory wipe facility enabled;

(t) effective logs and audit trails to identify abuses. Employees should be informed that such trails are in place.

(u) back-up systems. The Data User should determine the appropriate frequency and nature of back-up.

Organizational Security

(v) incident response plans. The Data User should anticipate what it would do if there were a data breach and be ready to respond.

Example: *Some issues the airline may address are:*

- *What would your organization do if there was a data breach incident?*

- *Is there a policy in place that specifies what a data breach is? (It may include any loss of control over Personal data, including inappropriate access on the organization's systems or the sending of Personal Data to the wrong parties)*
- *How would you know if the organization has suffered a data breach? Do employees at all levels understand the implications of losing Personal Data?*
- *Has your organization identified whom employees should report to if they have lost control of Personal Data?*
- *Does your policy make clear who is responsible for dealing with an incident?*

2.75 The Data User should periodically review its security practices in order to detect weaknesses in the organization and anticipate potential security breaches. Records of the Data User's policies, review and training should be kept.

2.76 In respect of transfers of Personal Data, the Data User should:

(a) ensure that it has obtained the written consent of its top management to transfer Personal Data using:-

(i) removable media devices (such as portable external storage devices); or

(ii) cloud computing services.

(b) record all transfers of Personal Data using removable media devices and/or cloud computing services.

(c) ensure that transfers of Personal Data by conventional means such as by post, by hand, fax and etc are recorded.

2.77 The Data User should periodically review its security practices in order to detect weaknesses in the organization and anticipate potential security breaches. Records of the Data User's policies, review and training should be kept.

Dealing with Disclosures to Data Processors

2.78 The Data User must also ensure that it has entered into a contract with the Data Processor to protect the Personal Data from loss, misuse, modification, unauthorised access and disclosure. **Appendix 5: Personal Data Disclosed or Received From Third Parties** sets out some example clauses which the

Data User may include in its agreement with Data Processors where Personal Data is disclosed to the Data Processor. These include:-

(a) confidentiality, non-disclosure and security requirements;

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

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

(d) security measures governing the processing to be carried out as may be contained in the Data User's internal security policy and the Standards.

In Practice

2.79 Data Users are required to develop and implement a security policy pursuant to the Regulations.

(F) Retention Principle (Section 10 of the PDPA)

2.80 Under the retention principle, Data Users should only keep Personal Data for as long as necessary to fulfil the purpose of processing. Upon the fulfilment of the purpose, Data Users are required to permanently destroy or delete all manual and electronic versions of the Personal Data.

How to Comply with the Retention Principle?

2.81 Some of the steps a Data User may take to comply with the Retention Principle include but are not limited to the following:-

(a) Identity all legislation related to the processing and retention of Personal Data prior to destroying any Personal Data

(b) Personal Data should not be kept longer than is necessary for any purposes unless there are legal provisions that require longer retention of Personal Data

The PDPA does not override the provisions of other law that require the retention of information or documents for a specific duration. For example, the Companies Act 1965, Income Tax Act 1967, Employment Act 1955, Sabah Labour Ordinance, Sarawak Labour Ordinance, the Limitation Act 1953, Sarawak Limitation Ordinance, and Sabah Limitation Ordinance (Cap 72)

require documents to be kept for a certain length of time. The PDPA and other applicable laws must be read together.

(c) The Data User must dispose Personal Data collection forms used for commercial forms within 14 days, unless the forms have legal value attached to the commercial transaction.

Data Users must delete Personal Data collection forms within fourteen (14) days of use, unless the Data User can justify the value for retaining the forms. For example, the collection forms may be needed for the purposes of the transaction which is not yet completed.

(d) The Data User should not use removable media devices to store Personal Data without the written consent of top management.

Data Users should prohibit the use of pen drives or external hard disks without written authority from authorized personnel.

(e) The Data User must review and delete Personal Data that is no longer needed from the database.

(f) The Data User must adopt a Personal Data disposal schedule to dispose Personal Data as which has been inactive for a period of twenty-four (24) months. The Data User must record this schedule of disposal.

Data Users should implement a periodical schedule of review and disposal of Personal Data and record its review and disposal procedures.

(g) The Data User should maintain records on the disposal of Personal Data which should be submitted as directed by the Commissioner.

How long can Personal Data be retained?

2.82 The PDPA does not specify the acceptable duration for which Personal Data may be kept. It is therefore subject to the Data User to keep Personal Data for as required under the statutory law and / or in accordance with company policy.

2.83 Personal Data may be retained permanently if such retention is necessary for:

(a) legal proceedings or a regulatory or similar investigation or obligation to produce the said information;

(b) a crime is suspected or detected; or

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

This requirement applies to both manual and electronic copies of documents containing Personal Data.

Destruction / Deletion of Personal Data

2.84 The Data User is required to **permanently** destroy or delete all physical and electronic versions of Personal Data.

Example: *An employee may permanently destroy physical copies of Personal Data by shredding all paper copies. Electronic versions of Personal Data may be permanently deleted by using secure deletion software, or restoring mobile devices to factory settings.*

2.85 Where a Data User needs to keep Personal Data beyond a specific statutory period, it should show a reasonable need for this.

Example: *The commencement of legal proceedings or investigations concerning the Data Subject is a legitimate reason for continuing to retain the Personal Data until the disposal/closure of the matter.*

2.86 As an alternative to destroying or permanently deleting Personal Data, Data Users may anonymize Personal data. Anonymized Personal Data is not considered Personal Data under the PDPA as it will not be able to be linked to any particular Data Subject.

Example: *Data Users may delete identifying information such as names, e-mail addresses, phone numbers, home addresses or passport and identity card numbers.*

In Practice

2.87 To implement sound retention practices, the Data User should develop standard operating procedures for Personal Data retention and disposal practices. Identified employees should be trained to implement such procedures.

(G) Data Integrity Principle (Section 11 of the PDPA)

2.88 The Data Integrity Principle requires Data Users to take reasonable steps to ensure that Personal Data is accurate, complete, not misleading and kept up-to-date:

(a) having regard to the purpose for collecting and processing the Personal Data; and

(b) any directly related purpose.

2.89 The Data User must take reasonable steps to ensure that Personal Data is:

(a) accurate in the sense that the Personal Data is captured correctly.

(b) complete in the sense that there is no omission of details in the Personal Data. The information recorded by the Data User must correctly reflect the information given by the Data Subject.

(c) not misleading in the sense that Personal Data should not be ambiguous, deceiving or an oversight. For example, the marital status of the Data Subject should not be falsely reflected by the Data User.

(d) kept up-to-date in the sense that the Data User should ensure that the Personal Data is the latest data given by the Data Subject. For example, the change of address made by the Data Subject must be recorded by the Data User.

What are "reasonable steps"?

2.90 The Data User may take "reasonable steps" to comply with the Data Integrity Principle, including but not limited to:-

(a) provide forms which the Data Subject may complete to update Personal Data whether in electronic or physical form;

(b) update Personal Data immediately after receiving a Data Correction Request from a Data Subject;

(c) ensure that relevant laws are complied with in determining the types of supporting documents required to determine the validity of the Data Subject's Personal Data.

(d) inform Data Subjects on their ability to update Personal Data whether through a portal or by displaying a notice on the Data User's premises or other suitable means.

(e) other reasonable steps according to the purpose of why the Personal Data was collected.

Example: *Where Personal Data is retained by the Data User for the purposes of providing flight information purchased by the Data Subject, issuing promotions, latest information updates or upgrades to the Data Subject, it is reasonable for the Data User to ensure that the Personal Data remains correct by way of verifying the Personal Data based on official identification documents from the Data Subject. However, it is unreasonable to expect the Data User to ensure that the address of the Data Subject is always kept up-to-date.*

Example: *The Data User may remind the Data Subject to update the Personal Data by notifying the Data Subject through email and/or on the Data User's corporate websites. But it is the responsibility of the Data Subject to notify the Data User of any changes to the Personal Data.*

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

(a) The Data User may require the Data Subject to inform the Data User of any change to his/her Personal Data. This is so that the Data User will not be in breach of the Data Integrity Principle if the Data User is not informed by the Data Subject of changes to his/her Personal Data.

(b) The Data User should enable Data Subjects to submit Data Correction Requests to update or correct his/her Personal Data at the Data User's branches and/or corporate website and at other points of contact with Data Subject.

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

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

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

2.95 The Data User is not required to update or correct his/her Personal Data based on information given by any party other than the Data Subject.

2.96 The Data Integrity Principle will not be breached if:

(a) a Data User retains Personal Data which is historical in nature (for example, the previous address or contact number of the Data Subject); and

(b) a Data User retains Personal Data that records events that happened in error (for example, where a Data Subject's account was accidentally terminated but has since been reinstated, the Data User is permitted to retain all records as it accurately reflect the error).

Right to Correct Personal Data (Section 34 of the PDPA)

2.97 The Data Subject is entitled to request that Personal Data held by the Data User be corrected where he or she considers that the Personal is inaccurate, incomplete, misleading or not up-to-date.

Exemptions

2.98 The Data User is not required to comply with a DCR where Personal Data is processed:

(a) for the prevention or detection of crime or for the purpose of investigations;

(b) for the apprehension or prosecution of offenders;

(c) for the assessment or collection of any tax or duty or any other imposition of a similar nature;

(d) for the preparation of statistics or carrying out research, provided that Personal Data is not processed for any other purpose and the resulting statistics or results of research are anonymised;

(e) for the purpose of or in connection with any order or judgement of a court; or

(f) for the purpose of discharging regulatory functions.

How Does a DCR work?

2.99 The Data Subject makes a DCR in writing to the Data User.

2.100 Upon receiving the DCR, the Data User must acknowledge receipt of the request.

2.101 After acknowledging receipt and verifying that the DCR is complete, the Data User must make the necessary correction to the Personal Data and supply a copy of the corrected Personal Data to the requestor within twenty-one (21) days after the date of receipt of the DCR.

2.102 The Data User must then take reasonable steps to supply relevant Third Parties with the updated Personal Data with a written notice on the reasons for correction.

2.103 Once the period of twenty-one (21) days has lapsed and the Data User is unable to comply within this period, the Data User:

(a) must notify the Data Subject in writing of the delay and the reasons for the delay and an extension of not more fourteen (14) days is automatically granted to the Data User; **or**

(b) must notify the Data Subject if it has grounds for refusing to comply with the DCR.

2.104 If 2.103(a) applies, the Data User must comply with the DCR within this fourteen (14) day extension period.

What are the requirements for a valid DCR?

2.105 The PDPA does not specify a particular format for the DCR. However, it must:

(a) be in writing;

(b) be enclosed with payment stipulated under the Fees Regulations, unless waived by the Data User;

(c) contain the necessary information to require the Data User to locate the Personal Data. For example, the Data Subject may provide information on the name, NRIC or passport number, address, account number;

(d) be specific as to the Personal Data to be corrected;

(e) where a request is made on behalf of the Data Subject, certified documentation will need to be submitted in order to establish the Data Subject's right to make a request.

2.106 If any of these requirements are not fulfilled, the Data User should return the DCR to the Data Subject and ask for the omitted requirements to be resubmitted.

What if I receive a verbal request?

2.107 Data Users are not required to respond to verbal requests. However, Data Users may choose to guide the Data Subject on the proper manner of making the DCR.

Can persons make a DCR on behalf of the Data Subject?

2.108 A DCR may be made on behalf of the Data Subject. In particular:

(a) where the Data Subject is below 18 years of age, the parent, guardian or person who has parental responsibility for the Data Subject may make the DCR;

(b) where the Data Subject is incapable of managing his own affairs, a person appointed by a court to manage the Data Subject's affairs or a person authorized in writing by the Data Subject may make the DCR; or

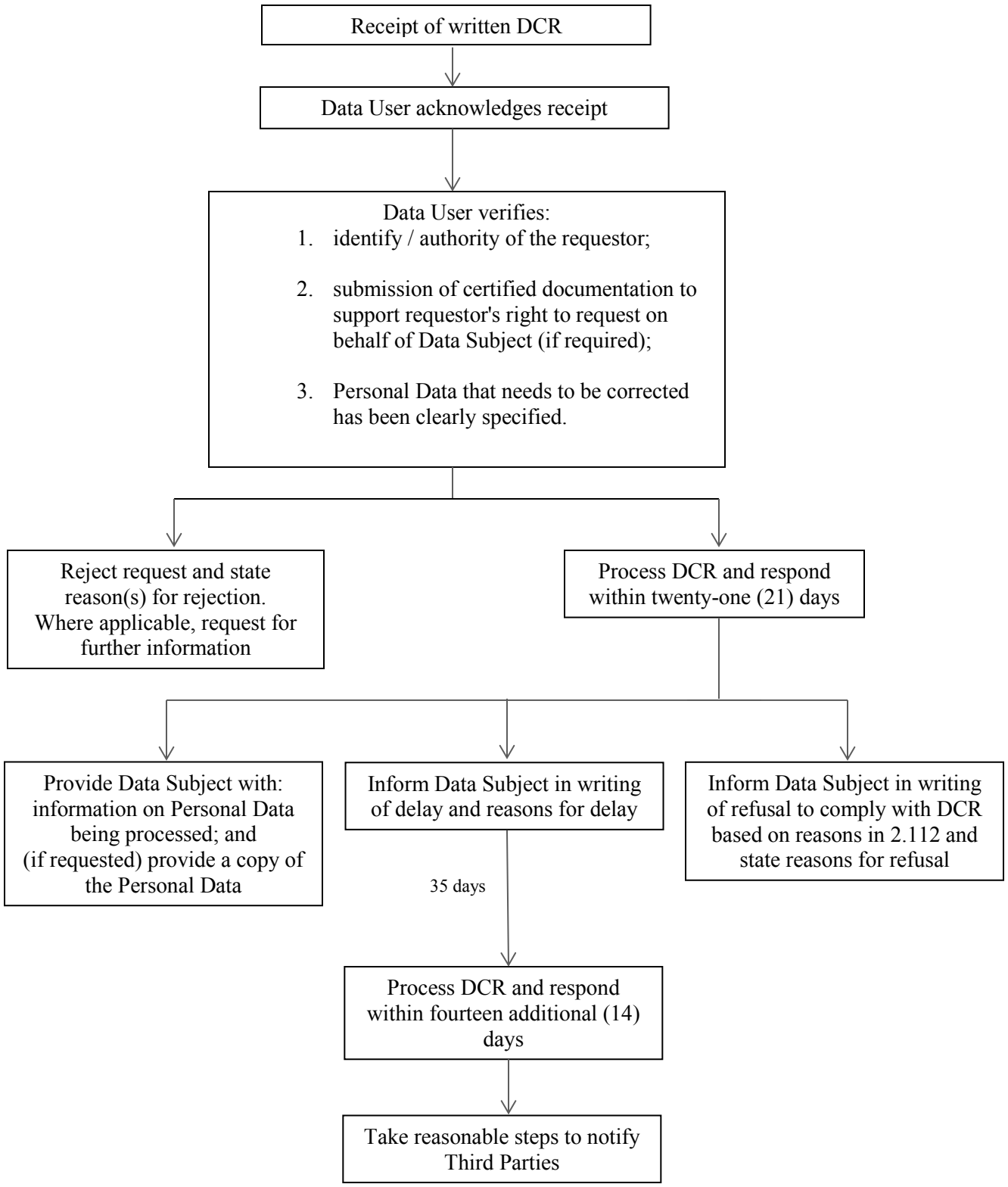
(c) in any other case, a person authorized in writing by the Data Subject to make a DCR on behalf of the Data Subject.

What about Personal Data held by Third Parties?

2.109 Where Personal Data has been disclosed to a Third Party during the twelve (12) months preceding the day the DCR is received, and the Third Party has not ceased using the Personal Data, the Data User must take reasonable steps to provide a copy of the updated Personal Data to the Third Party.

What is the procedure for processing a DCR?

2.110 The flow chart below shows the steps a Data User should take upon receiving a DCR.



2.111 If the Data User is only able to correct some of the Personal Data requested, the Data User must provide the Data Subject with the corrected Personal Data to the extent it is able to do so.

When may a Data User refuse a DCR?

2.112 The Data User has the right not to comply with or to reject a DCR if:

(a) Inability to verify identity

the Data User is not supplied with necessary information as the Data User may reasonably require (such as, the Data Subject's name, identification card number, address and other information as the Data User may determine);

(b) Inability to verify need for correction

the Data User is not supplied with sufficient information, as the Data User may reasonably require, to determine how the Personal Data is inaccurate, incomplete, misleading or not up-to-date;

Example: *The Data Subject submits a DCR to correct his/her name but does not provide supporting documents for his/her request.*

(c) Personal Data does not need correction

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

(d) DCR inaccurate

the Data User is not satisfied that the correction requested is accurate, complete, not misleading or up-to-date.

Example: *Where a Data Subject seeks a change to his or her home address but the Data User has grounds to believe that the new address provided is an attempt to avoid the service of a summons on the Data Subject.*

2.113 The Data user may request for supporting evidence prior to correcting the Personal Data.

What if I receive a request to correct an expression of opinion?

2.114 Where the DCR relates to an expression of opinion held by the Data User and the grounds above do not apply, the Data User may disagree that the said expression of opinion is inaccurate, incomplete, misleading or not up to date. However, the Data User must:

(a) make a note on how the expression of opinion is considered by the requestor to be inaccurate, incomplete, misleading or not up to date;

(b) annex the note to the Personal Data in question (for example, annexing the note to the physical file containing the Personal Data) or maintain the note separately;

(c) ensure that the note is brought to the attention of any person who wishes to use the expression of opinion and ensure that the note is available for inspection; and

Example: *The note may be inserted as a system pop-up to notify the person accessing the Personal Data of the differing opinions regarding the Personal Data in question.*

(d) attach a copy of the note to the written notice informing the Data Subject of the Data User's refusal to comply with the DCR.

Can I charge fees?

2.115 The Data User is not entitled to charge fees for DCRs.

Keeping Records

2.116 Data Users should maintain a record of all DCRs received and the decisions made on complying or not complying with each DCR. This will enable the Data User to answer any query from the Data Subject and/or prepare the Data User in the event of an investigation by the Commissioner.

2.117 As a matter of good practice, the Data User should maintain a file for each DCR with the following information:

(a) a copy of the DCR;

(b) a record of the verification of the identity of any authorised person making a request on the Data Subject's behalf;

(c) copies of all correspondences relating to the DCR;

(d) a record of any decision made in relation to the DCR; and

(e) a copy of the corrected Personal Data that was sent to the Data Subject or authorized person.

2.118 A sample DCR Form is provided in **Appendix 6: Data Access Request / Data Correction Request Form.**

In Practice

2.119 It is recommended that the Data User implements policies and procedures with regard to the methods in which it will ensure that Data Subjects have a way of contacting the Data User to correct their Personal Data.

(H) Access Principle (Section 12 of the PDPA)

2.120 Under the Access Principle, the Data Subject has the right to request access to his/her Personal Data and the right to correct his/her Personal Data which is inaccurate, incomplete, misleading or not up-to-date.

2.121 The Data User is required to respond to any Data Access Request ("**DAR**") in order to comply with the PDPA.

2.122 The Data Subject may only access his/her own Personal Data. Data Subject must not be granted access to another person's Personal Data, except as set out under this Code.

2.123 Data User has the right to refuse any DAR submitted by the Data Subject. Data Users may charge an appropriate fee for addressing these requests. These are further elaborated below.

Exemptions

2.124 The Data User is not required to comply with a DAR where Personal Data is processed:

(a) for the prevention or detection of crime or for the purpose of investigations;

(b) for the apprehension or prosecution of offenders;

(c) for the assessment or collection of any tax or duty or any other imposition of a similar nature;

(d) for the preparation of statistics or carrying out research, provided that Personal Data is not processed for any other purpose and the resulting statistics or results of research are anonymised;

(e) for the purpose of or in connection with any order or judgement of a court; or

(f) for the purpose of discharging regulatory functions.

How Does a DAR work?

2.125 The Data Subject makes a DAR in writing to the Data User. The DAR may be to:

(a) seek information on the Personal Data being processed by the Data User; or

(b) to have communicated to the Data Subject a copy of the Personal Data in an intelligible form. The Data Subject must be able to understand the information supplied without having to go back to the Data User for an explanation.

2.126 Upon receiving the DAR, the Data User must acknowledge receipt of the request.

2.127 After acknowledging receipt and verifying that the DAR is complete, the Data User must deliver the information requested and/or a copy of the Personal Data to the Data Subject (if required) within 21 days after the date of receipt of the DAR.

2.128 Once the period of 21 days has lapsed and the Data User is unable to comply within this period, the Data User:

(a) must notify the Data Subject in writing of the delay and the reasons for the delay and an extension of not more fourteen (14) days is automatically granted to the Data User; **or**

(b) must notify the Data Subject if it has grounds for refusing to comply with the DAR.

2.129 If 2.128(a) applies, the Data User must comply with the DAR within this fourteen (14) day extension period.

What are the requirements for a valid DAR?

2.130 The Regulations provide that where a Data Subject does not require a copy of the Personal Data, the Data Subject must inform the Data User in writing upon submitting the DAR. To facilitate this, it is recommended that the Data User provides the Data Subject with a choice at the point of making the DAR as to whether the Data Subject:

(a) merely wishes to confirm whether or not the Data User retains any Personal Data of the Data Subject and the type of Personal Data held by the Data User; or

(b) wishes to be provided with a copy of the Personal Data held by the Data User.

2.131 The PDPA does not specify a particular format. However, it must:

(a) be in writing;

(b) be enclosed with payment stipulated under the Fees Regulations, unless waived by the Data User;

(c) contain the necessary information to require the Data User to locate the Personal Data. For example, the Data Subject may provide information on the name, NRIC or passport number, address, account number;

(d) be specific. A request for "all Personal Data" will not be considered to be a proper DAR;

(e) where a request is made on behalf of the Data Subject, certified documentation will need to be submitted in order to establish the Data Subject's right to make a request.

2.132 If any of these requirements are not fulfilled, the Data User should return the DAR to the Data Subject and ask for the omitted requirements to be resubmitted.

What if I receive a verbal request?

2.133 Upon receiving a verbal request, the Data User should guide the Data Subject on the proper manner of making the DAR.

Can persons make a DAR on behalf of the Data Subject?

2.134 A DAR may be made on behalf of the Data Subject. In particular:

(a) where the Data Subject is below eighteen (18) years of age, the parent, guardian or person who has parental responsibility for the Data Subject may make the DAR;

(b) where the Data Subject is incapable of managing his own affairs, a person appointed by a court to manage the Data Subject's affairs or a person authorized in writing by the Data Subject may make the DAR; or

(c) in any other case, a person authorized in writing by the Data Subject to make a DAR on behalf of the Data Subject.

What if I receive a DAR for multiple accounts?

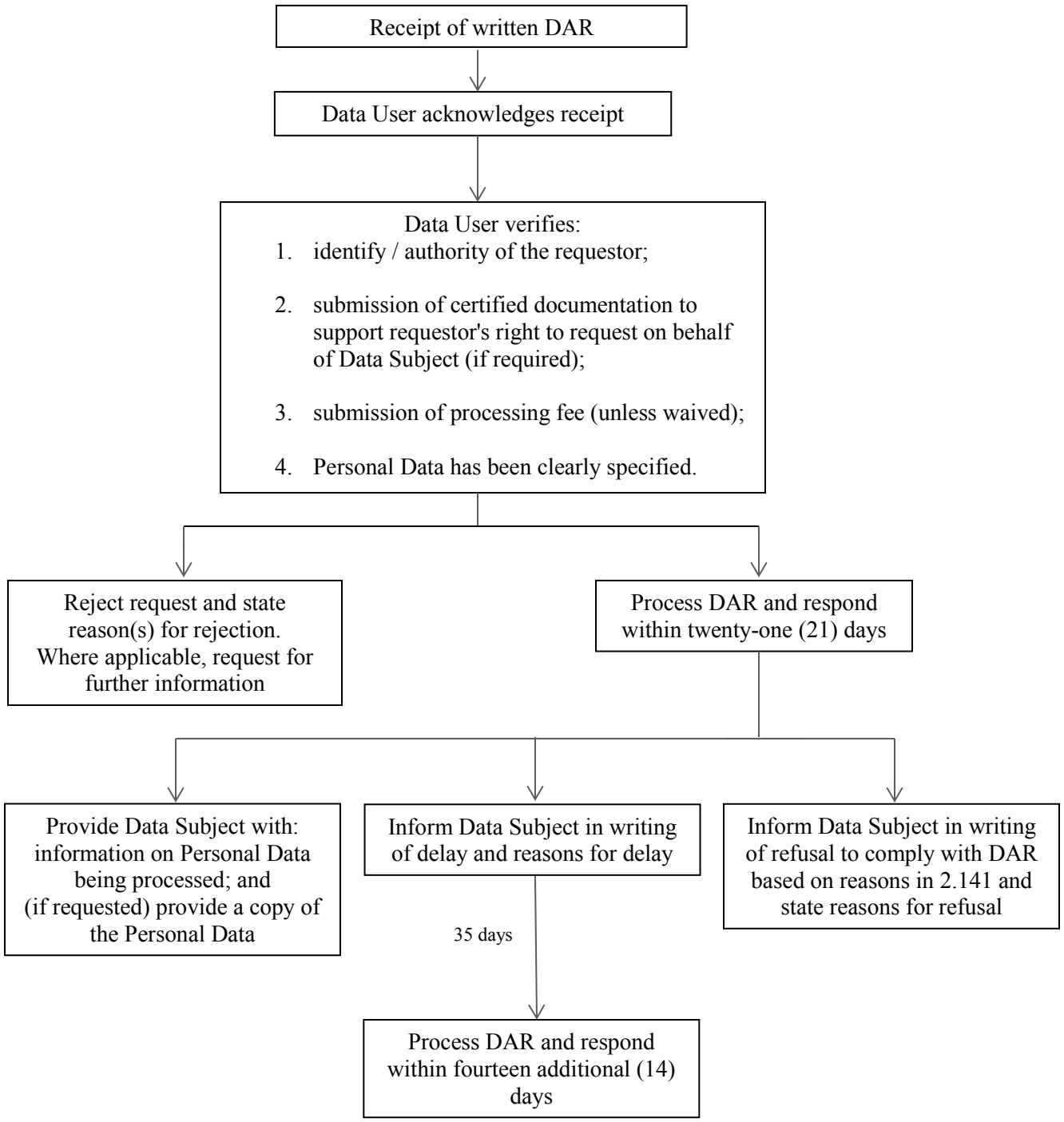
2.135 Where a Data Subject has separate accounts with a Data User, the Data User may require separate DARs for each account.

What about archived Personal Data?

2.136 The Data Subject does not have a right of access to Personal Data maintained for backup and archival purposes.

What is the procedure for processing a DAR?

2.137 The flow chart below shows the steps a Data User should take upon receiving a DAR.



2.138 If the Data User is only able to locate some of the Personal Data requested, the Data User must provide the Data Subject with the Personal Data to the extent it is able to do so.

2.139 Where the Personal Data is contained within a video or audio, the Data User may:

(a) communicate audio recordings as written transcript or provide the Personal Data in audio form (e.g .wmv or mpeg); or

(b) communicate video recordings (including CCTV stills) as a chronological set of images or as an edited video recording where the identities of third parties are masked.

What happens if a Data User does not comply with a DAR?

2.140 A Data Subject has the right to lodge a complaint with the Commissioner in the event the Data User does not comply with a DAR. However, a Data User may refuse to comply with a DAR if it has legitimate reasons to do so, as recognised under the PDPA.

When may a Data User refuse a DAR?

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

(a) Inability to verify identity

The Data User is not provided with necessary information as the Data User may reasonably require (for example, Data Subject's name, identification card number, address, and such other related information as the Data User may determine) in order to establish the identity of the Data Subject or where the DAR is submitted by an authorised person, establish that person's connection to the Data Subject;

(b) Inability to verify location of Personal Data

The Data User is not supplied with sufficient information by the Data Subject to determine the exact location of the Personal Data;

(c) Disproportionate burden

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

(d) Disclosure of another

The Data User is unable to comply with the DAR without Disclosing another person's Personal Data. In such a situation, the Data User may:

(i) anonymise the third party Personal Data;

(ii) seek consent of the third party if practical; or

(iii) determine whether or not it will be reasonable to disclose the Personal Data without the third party's consent.

(e) Court Order

Providing access which would violate a court order;

(f) Confidentiality

Providing access which would disclose confidential commercial information;

(g) Regulation

Such access is regulated by a law other than the PDPA, (for example, the Malaysian Aviation Commission Act 2015); or

2.142 Where the Data User has grounds for refusal, the Data User may choose to refuse to provide all or some of the Personal Data, depending on the circumstances.

Can I charge fees?

2.143 Pursuant to the Fees Regulations, the Data User is entitled to charge the Data Subject for each DAR submitted. The maximum fees payable by a Data Subject for the submission of a DAR are:

Item	Description	Maximum fee (RM)
(a)	For Personal Data with a copy	10
(b)	For Personal Data without a copy	2
(c)	For Sensitive Personal Data with a copy	30
(d)	For Sensitive Personal Data without a copy	5

Keeping Records

2.144 Data Users should maintain a record of all DARs received and the decisions made on complying or not complying with each DAR. This will enable the Data User to answer any query from the Data Subject and/or prepare the Data User in the event of an investigation by the Commissioner.

2.145 As a matter of good practice, the Data User should maintain a file for each DAR with the following information:

(a) a copy of the DAR;

(b) a record of the verification of the identity of any authorised person making a request on the Data Subject's behalf;

(c) copies of all correspondences relating to the DAR;

(d) a record of any decision made in relation to the DAR; and

(e) a copy of the Personal Data that was sent to the Data Subject or authorized person.

2.146 A sample DAR Form is provided in **Appendix 6: Data Access Request / Data Correction Request Form.**

3.0 Rights of the Data Subject

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

3.1 The Data Subject may, via a written notice, require the Data User to:

(a) cease processing the Personal Data; or

(b) not begin the processing of Personal Data,

where the processing is causing or is likely to cause substantial and unwarranted damage or distress to the Data Subject or another person.

What is "substantial" or "warranted"?

3.2 "Substantial damage", "substantial distress" and "unwarranted" are not defined under the PDPA. However, in most cases:

(a) “substantial damage” includes financial loss suffered by the Data Subject;

(b) “substantial distress” includes emotional or mental trauma suffered by the Data Subject; and

(c) “unwarranted” means that the damage or distress suffered by the Data Subject is not justifiable.

When may a request be refused?

3.3 The Data Subject does not have the right to prevent processing where:

(a) the Data Subject has consented to the processing; or

(b) the processing is necessary;

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

(ii) to take steps at the request of the Data Subject with a view to entering into a contract;

(iii) for compliance with legal obligations that apply to the Data User, other than a contractual obligation; or

(iv) to protect the Data Subject’s vital interests, such as matters relating to life, death or the security of a Data Subject.

What are the timelines which the Data User must follow?

3.4 Upon receiving a written notice to cease processing or not to commence processing of Personal Data, the Data User must provide a written notice to the Data Subject within twenty-one (21) days of receiving such notice stating:

(a) that the Data User has complied or intends to comply with the said notice;

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

(c) where applicable, states his reasons for regarding the request as unjustified, and the extent if any, to which he has complied or intends to comply with the request.

How should a Data User assess such requests?

3.5 The Data User may consider the following when making a decision on whether to comply with the request:

(a) Are there legitimate reasons for the Data Subject's request? The Data Subject should provide legitimate reasons as the damage or distress caused must be "substantial".

(b) Is the damage or distress unwarranted? This is tied to whether the Data Subject has provided legitimate reasons for the request.

Rights of the Data Subject

3.6 Where the Data User does not comply with the notice, the Data Subject may apply to the Commissioner to require the Data User to comply with the notice.

3.7 If the Commissioner is satisfied that the Data Subject's request is justified, the Commissioner may require the Data User to comply with the request.

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

3.8 The Data Subject has the right to, via a written notice, require the Data User to cease or not begin processing Personal Data for the purposes of direct marketing. Part B, Chapter 5 further elaborates on the practices of the aviation sector in respect of direct marketing.

3.9 The Data User must comply with such a request within a reasonable time frame.

3.10 The Data Subject's written request must be communicated throughout the organisation to ensure that the Data Subject's request is followed. Where there is a need for the Data User to update relevant systems and databases to reflect the Data Subject's instructions, Data Users are, under normal circumstances, expected to comply with the Data Subject's request within three (3) months.

3.11 Where Data Subjects make a written request asking to receive some direct marketing materials and not others, the Data User may choose not to provide the Data Subject with all direct marketing materials, should their systems be incapable of distinguishing between the different types of direct marketing materials.

Dealing with Direct Marketing

3.12 Direct marketing is defined as "the communication by whatever means of any advertising or marketing material which is directed to a specific customers".

3.13 Data Users collect a wealth of personal information. The processing of vast amounts of information by the Data User leads to the potential for cross-selling and behavioural targeting to take advantage of previously unexplored areas of generating revenue.

3.14 Direct marketing must consist of advertising or marketing material **directed to a specific customers**. Marketing materials which are not directed to particular individuals but are instead sent to all customers of a Data User will not be considered as direct marketing.

***Example**: Displaying banners of promotional offers on the airline's customers which may be seen by the airline's potential customers using the airline's website.*

What are the requirements for direct marketing under the PDPA?

3.15 The Commissioner has not issued formal guidelines on dealing with direct marketing. However, it is recommended that Data Users adhere to the following practices:

Consent

(a) Data Users must obtain the consent of the Data Subject to use their Personal Data for direct marketing through postal mail. For direct marketing through electronic means, the Data Subject must give his / her **explicit consent**. **Appendix 3: General Principle** sets out template consent language for direct marketing.

Opt-Out

(b) The PDPA provides that the Data Subject has the right to withdraw consent to processing for direct marketing. The Data User must ensure that Data Subjects are able to withdraw consent at any time:

(i) Data Subjects should have the option to opt-out of direct marketing at the time of initial collection, through, for example, an opt-put tick-box;

(ii) the right to opt-out must be available on every subsequent marketing message. For example, the Data Subject may be provided with a link which he / she may click to "unsubscribe" to further marketing communications; and

(iii) the Data User's Privacy Notice should clearly provide other methods in which the Data Subject may contact the Data User to withdraw their consent to direct marketing.

It is recommended that Data Users develop a system to manage such refusal requests in order to ensure that all refusal requests are accurately captured and marketing materials are not sent to these Data Subjects. Data Users may also develop standard operating procedures and policies relating to managing such requests.

Source of Personal Data

(c) the Personal Data must have been obtained in the course of previous business dealings with the Data Subject, such as the sale of products or services.

Informed

(d) The Data Subject must have been informed of the identity of the Data User, that the Data Subject's Personal Data would be used for direct marketing, and whether the Personal Data may be disclosed to other third parties in relation to the direct marketing.

Similar Products / Services

(e) The direct marketing must be limited to similar products and services.

Can I obtain Personal Data from publicly available sources?

3.16 Data Users should not use Personal Data obtained from publicly available sources such as information found on Facebook or the internet for the purpose of direct marketing as the Data Subject would not have made such information publicly available for the purpose of receiving unsolicited direct marketing communications and has not provided his / her consent to receiving such communications.

Can I appoint a third party to conduct direct marketing on my behalf?

3.17 The Data User may appoint a third party Data Processor to conduct direct marketing on its behalf. However, it should ensure that an agreement is in place between the Data User and the Data Processor. Airlines may use the sample clauses provided in **Appendix 5: Personal Data Disclosed or Received From Third Parties.**

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

3.18 The Data Subject may withdraw his or her consent to the processing of Personal Data at any time by providing the Data User with a written notice.

3.19 The Data User must cease processing the Personal Data of the Data Subject upon receipt and confirmation of such notice. However, the Data User is not required to cease processing to the extent where the withdrawal of consent would affect the Data User's rights and obligations under contract or law.

***Example**: Such rights and obligations include:*

(a) the right to be paid for services rendered, for example, the settlement of bookings or tax invoices, or overdue payments;

(b) the right to bring and maintain legal proceedings against the Data Subject(For example: Where a passenger has lodged a complaint or commences legal proceedings against the airline, the airline may wish to retain Personal Data in order to ensure that it has a complete record of the transaction, which record may include Personal Details (eg. name, passport/IC number, address etc);

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

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

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

4.0 Specific Issues

(A) Managing Transfers of Personal Data Overseas

4.1 Data Users typically operate in several jurisdictions and may be required to transfer Personal Data to jurisdictions outside of Malaysia to, among others, partner airlines, overseas subsidiaries or back-up servers in other countries. The PDPA contains restrictions regarding the transfer of Personal Data overseas unless the Data Subject has consented to the transfer.

4.2 Where the Data Subject has not consented to the transfer, the PDPA permits transfers abroad where:

(a) the transfer is necessary for the performance of a contract between the Data User and the Data Subject;

(b) the transfer is necessary to perform or conclude a contract between the Data User and a third party which has been entered into at the request or in the interest of the Data Subject;

***Example**: Where Data User has to transfer Personal Data to a partner airline in order to ensure that connecting flights are available for a passenger's required journey.*

(c) the transfer is for legal proceedings or obtaining legal advice or for establishing, exercising or defending legal rights;

(d) the Data User has reasonable grounds for believing that in all circumstances of the case:

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

(ii) it is not practicable to obtain the consent in writing of the Data Subject to the transfer; and

(iii) if it was practicable to obtain such consent, the Data Subject would have given his / her consent.

(e) the Data User has taken all reasonable precautions and exercised all due diligence to ensure that Personal Data will not in the other jurisdiction be processed in contravention of the standards set out in the PDPA;

***Example**: The Data User has conducted due diligence on a selected third party services provider and entered into a data transfer agreement with the third party service provider.*

(f) the transfer is necessary in order to protect the vital interests of the Data Subject; or

(g) the transfer is necessary as being in the public interest as determined by the Minister.

In Practice

4.3 In order to be able to transfer Personal Data overseas, the most practical exception which Data Users may rely on is to obtain the consent of the Data Subject to such transfer. The consent may be obtained through the Privacy Notice and consent language. The Data User may do this by addressing the issue of transfers through the Privacy Notice and notifying the Data Subject that his / her Personal Data may be transferred overseas.

4.4 It is recommended that Data Users conduct due diligence on recipients of the Personal Data and ensure the appropriate warranties are obtained from the recipient of the Personal Data, such as:

(a) that the recipient provides all information and cooperation regarding the processing of Personal Data as the Data User may reasonably require to enable it to comply with the PDPA;

(b) to carry out processing only as required to fulfil the recipient's contractual obligations to the Data User;

(c) not to disclose the Personal Data to other persons except to the extent necessary to fulfil its contractual obligations to the Data User;

(d) to protect the security of the Personal Data and implement and maintain the necessary technological and organizational security measures and provide details of the same to the Data User if requested;

(e) not to retain the Data Subject's Personal Data for longer than is necessary to fulfil the recipient's contractual obligations to the Data User; and

(f) to permit the Data User and/or its representatives to conduct audits of the recipient's Personal Data processing facilities in order to ensure compliance with the PDPA.

(B) Miscellaneous

Can I take photos during corporate events?

4.5 Photographs contain images of a Data Subject which may identify a Data Subject. Such images are therefore likely to be Personal Data.

4.6 The Data User may take photos during a corporate event. However, the Data User should adopt the following practices:

(a) where the event is by invitation, the Data User should state on the invitation card that photographs will be taken and the images may be used for publication;

(b) if the event is open to the public, a clear notice should be placed at the entrance or reception of the venue to inform attendees that photographs will be taken at the event and that the images may be used for publication by the Data User.

What should I do if I contact the Data Subject but another person answers?

4.7 The Data User may on occasion be required to contact the Data Subject. If the call is received by a person other than the Data Subject, it is permissible for the Data User to inform the recipient of the call of the identity of the Data User, request for information on when the Data Subject would be available and state that the Data User will call back later.

4.8 The Data User must not disclose further details, such as any details relating to member I/D account, or any flight itinerary.

What about CCTV installations?

4.9 The Data User must display a notice visible to visitors of the premises informing the public of the CCTV operation and the purpose of the installation of CCTV.

4.10 The notice may:

(a) be in English and Bahasa Melayu;

(b) be visible and noticeable at all entry and exit points of the Data User's premises, especially within the CCTV surveillance zones; and

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

4.11 Data Users may use the following sample notice:

(a) In English

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

(b) In Bahasa Melayu

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

Displaying the Certificate of Registration

4.12 Airlines are required to obtain and display the original Certificate of Registration issued by the Commissioner at its headquarters.

4.13 At each of its branches, Data Users are required to display copies of the Certificate of Registration which has been certified by the Commissioner.

4.14 A branch means any office operated by the Data User where interaction occurs with the Data Subject. However, kiosks, exchanges and offices where there is no interaction with the Data User are not considered as "branches".

4.15 The Data User may display the Certificate of Registration on notice boards within the premises, on electronic displays and on the corporate website of the Data User.

5.0 Compliance in Practice

Maintaining a PDPA System

5.1 The Regulations provide that the Data User must maintain a personal data system which must be open for inspection by the Commissioner or relevant officer. The Data User must maintain:

(a) the record of consents from a Data Subject in respect of the processing of Personal Data by the Data User;

(b) the record of written notices issued by the Data User to the Data Subject;

(c) the list of disclosures to Third Parties in respect of Personal Data that has been or is being processed by that Third Party;

(d) the record of compliance in accordance with the Retention Standard;

(e) the record of compliance in accordance with the Data Integrity Standard; or

(f) such other related information.

Policies and Procedures

5.2 Implementing compliance involves the development of policies and procedures which prescribe dos and don'ts relating to Personal Data.

5.3 Further:

(a) these policies and procedures must be communicated to employees;

(b) relevant employees should be trained on the policies, procedures and made aware of the PDPA, the Standards and the Regulations. Employees should be provided with training on the PDPA and relevant data protection policies when they first join the company;

(c) Awareness of the relevant data protection policies should be part of every Data User's employee's ;

(d) the Data User should implement levels of authorization and restrict access to Personal Data to selected employees only;

(e) confidentiality clauses and possible sanctions for breach should be incorporated into the employment agreement or employment manual / handbook; and

(f) Data Users should develop protocols for steps to be taken pursuant to a security breach or breach of the PDPA by an employee.

5.4 Data Users are encouraged to ensure that appropriate training and/or awareness is put in place for employees to ensure that employees understand the importance of complying with these policies and procedures. Relevant employees may be identified to receive further specific training, such as training on security and fraud awareness and on handling data access / correction requests.

5.5 The Data User should ensure that it keeps up with the latest developments in the PDPA and continue to provide training to employees as and when required to keep up with any changes.

6.0 Administration of the Code

Compliance and Monitoring

6.1 The Data User must develop and implement appropriate compliance policies, procedures and a framework to ensure compliance with the PDPA and this Code.

6.2 In order to monitor compliance, Data Users are encouraged to:

(a) implement an internal monitoring framework; and

(b) conduct self-audits.

6.3 If the Data User identifies shortcomings and weaknesses in the implementation of the compliance framework, the Data User should ensure that the weaknesses or shortcomings are addressed as soon as reasonably possible.

6.4 It is recommended that the Data User:

(a) implement a reporting system by key persons within the organization (for example, the officers responsible for PDPA compliance, heads of business units and relevant key employees) to the senior management of the Data User, to review and assess the status of implementation of the PDPA and this Code. This will enable the Data User to monitor issues, address shortcomings and track the progress of the Data User in complying with the PDPA and the Code.

(b) conduct periodic self-audits to identify issues relating compliance with the PDPA and this Code.

6.5 Where required, Data Users should meet each other to discuss issues arising under the Code and other related matters.

Amendment

6.6 This Code may be amended, revised or updated to include all changes to the PDPA. The Commissioner will notify the Data User in writing of all amendments, revisions or updates to the PDPA.

6.7 Amendments to this Code may be made where:

(a) there are amendments to the PDPA, the Regulations and/or the Standards;

(b) the Commissioner makes amendments of his / her own accord; and/or

(c) the Data User makes recommendations for amendments to the Commissioner based on the results of the review of this Code.

6.8 The Commissioner will enter the particulars of amendments in the Register of Code of Practice and will make the same available to the public.

6.9 All amendments to the Code will be effective upon registration of the same in the Register of the Code of Practice.

7.0 Appendices

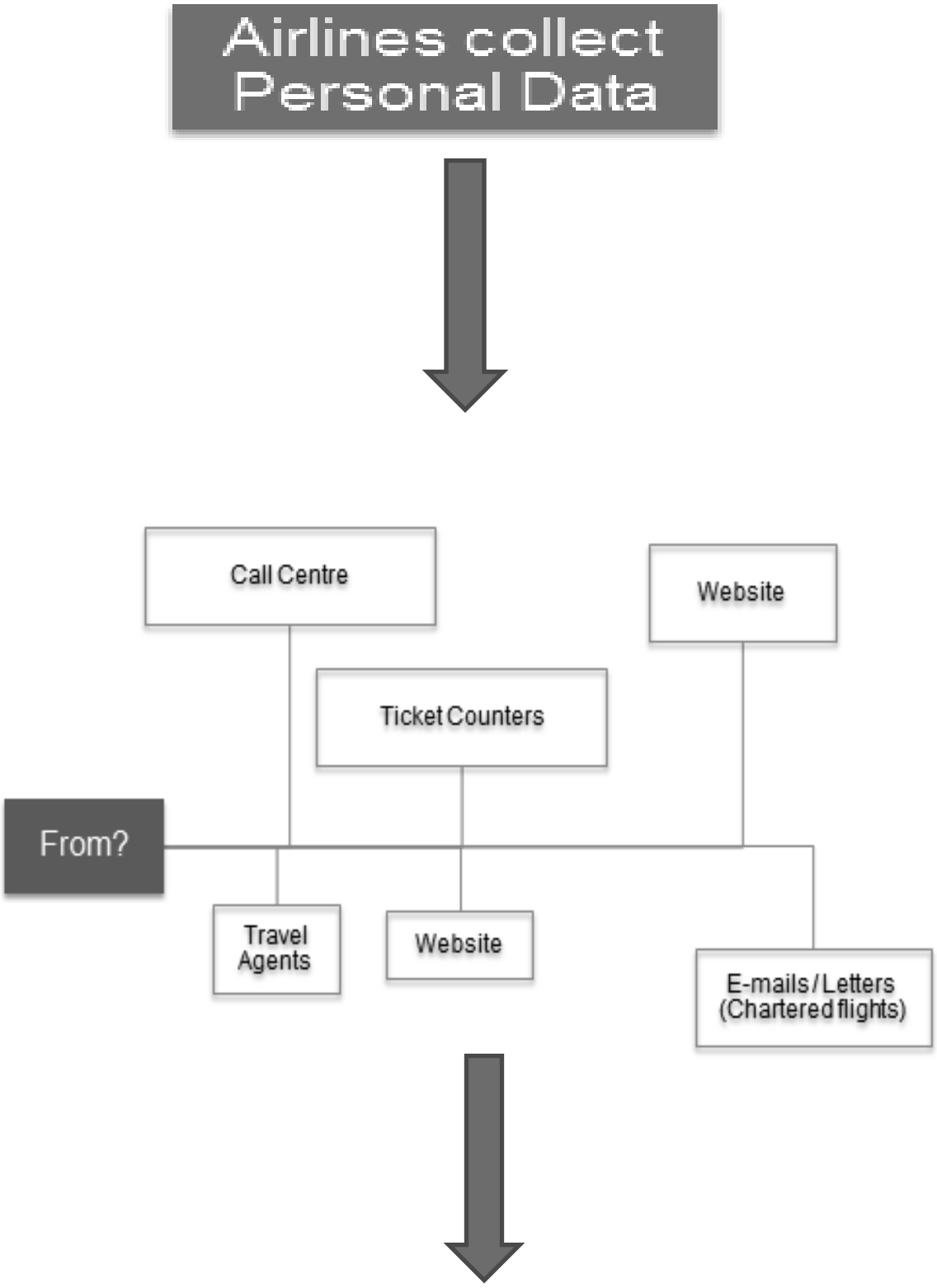
APPENDIX 1 - DEFINITIONS/GLOSSARY

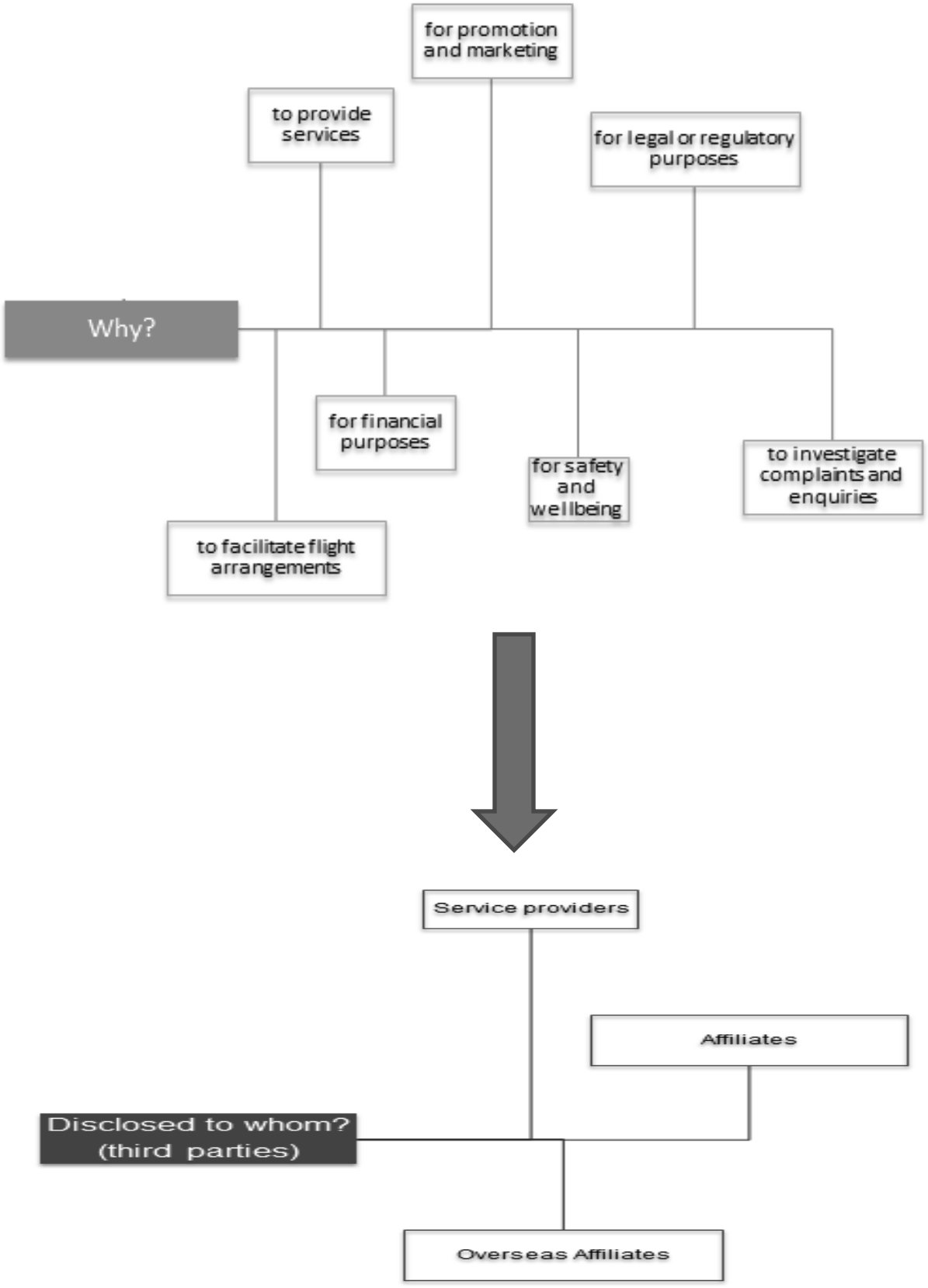
Words	**Definition**
Code	This Personal Data Protection Code of Practice for the Aviation Sector.
Collect	In relation to Personal Data, an act by which Personal Data enters into or comes under the control of a Data User.
Commercial transaction	Any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a credit reporting business carried out by a credit reporting agency under the Credit Reporting Agencies Act 2010.
Commissioner	The Personal Data Protection Commissioner appointed pursuant to the PDPA.
Data Access Request	Written request made by the Data Subject to the Data User to access Personal Data of that Data Subject.
Data Correction Request	Written request made by the Data Subject to the Data User to correct Personal Data of that Data Subject.
Data Processor	Any person, other than an employee of the Data User, who processes the Personal Data solely on behalf of the Data User, and does not process Personal Data for any of his own purposes.
Data Subject	A person who is the subject of Personal Data. Under this Code includes the following: (a) persons who are or who were customers of a Data User; (b) persons who represent customers of a Data User (such as parents of minors, trustees and authorized representatives); and (c) persons who have been identified as potential customers of a Data User.
Data User	A person who either alone or jointly or in common with other persons processes any Personal Data or has control over or authorizes the processing, but does not include a Data Processor. Under this Code:- (a) Malaysia Airlines Berhad; (b) AirAsia Berhad; (c) AirAsia X Berhad;

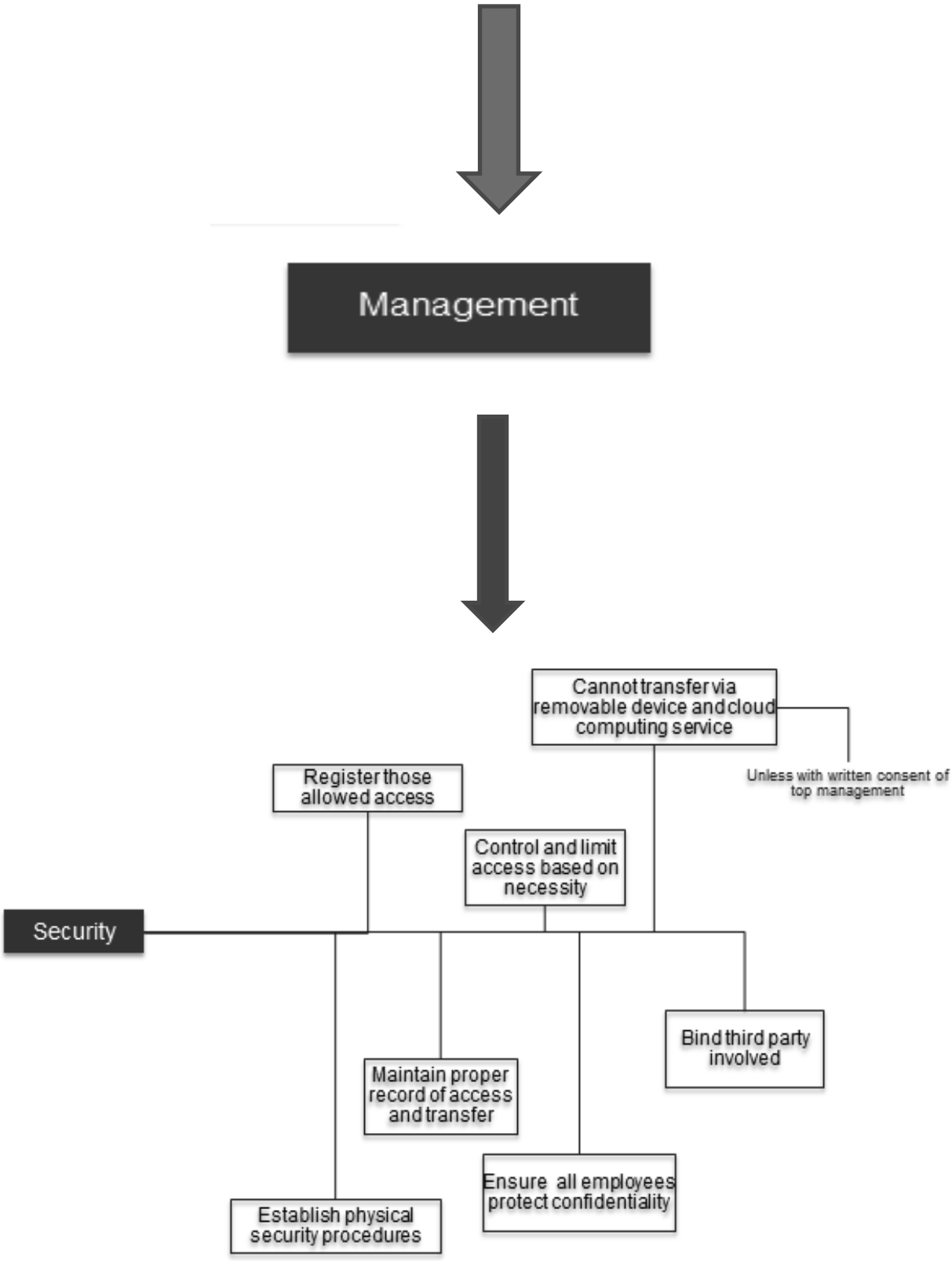
	(d) MASWINGS Sdn. Bhd. ; (e) Malindo Airways Sdn Bhd; (f) Berjaya Air Sdn Bhd; and (g) FlyFirefly Sdn Bhd.
Direct Marketing	Communication by whatever means of any advertising of any advertising or marketing material which is directed to particular persons.
Disclose	In relation to Personal Data, an act by which Personal Data is made available by a Data User.
Expression of Opinion	An assertion of fact which is unverifiable or in all circumstances of the case is not practicable to verify.
Fees Regulations	Personal Data Protection (Fees) Regulations 2013.
Opt-in	Refers to the positive choice made by a Data Subject to elect to receive or subscribe to services and/or marketing communications from the Data User.
Opt-out	Refers to positive act of a Data Subject of choosing to unsubscribe or not receive services and/or marketing communications which the Data Subject already receives due to a pre-existing relationship with the Data User..
PDPA	Personal Data Protection Act 2010
Personal Data	Any information in respect of Commercial Transactions, which: (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or (c) is recorded as part of a Relevant Filing System or with the intention that it should form part of a Relevant Filing System; that relates directly or indirectly to a Data Subject, who is identified or identifiable from that information or from that and other information in the possession of a Data User, including any Sensitive Personal data and expression of opinion about the Data Subject, but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.
Privacy Notice	Personal Data Protection Notice issue by a Data User, as may be amended by a Data User from time to time.

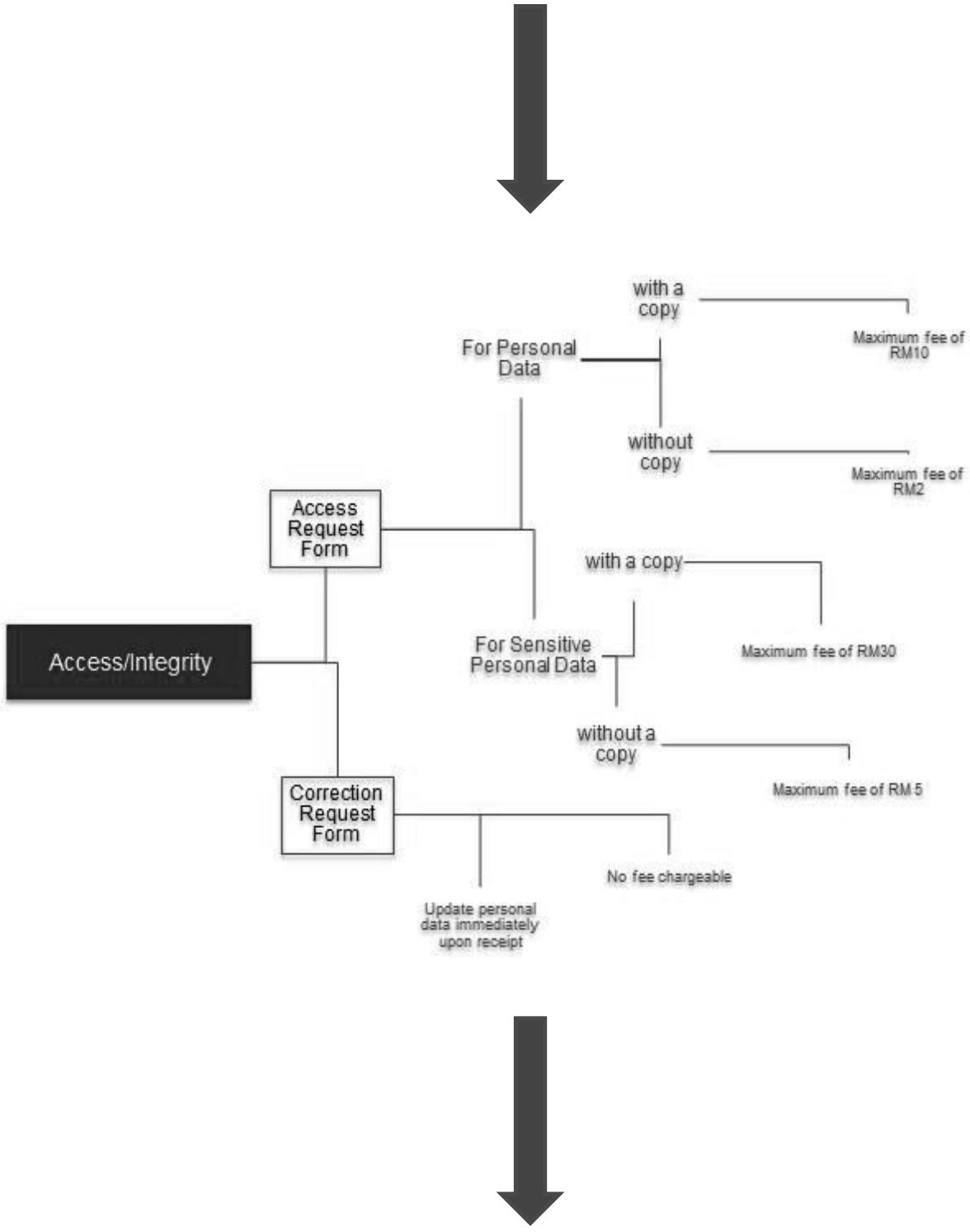
Process, Processes, Processed, Processing	In relation to Personal Data, means collecting, recording, holding or storing Personal Data or carrying out any operation or set of operations on Personal Data, including: (a) the organisation, adaptation or alteration of Personal Data; (b) the retrieval, consultation or use of Personal Data; (c) the disclosure of Personal Data by transmission, transfer, dissemination or otherwise making available; or (d) the alignment, combination, correction, erasure or destruction of Personal Data.
Regulations	Personal Data Protection Regulations 2013.
Relevant Filing System	Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set of information is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.
Sensitive Personal Data	Any Personal Data consisting of information as to the physical or mental health or condition of a Data Subject, his / her political opinions, his / her religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him / her of any offence or any other Personal Data that the Minister may determine by order published in the Gazette.
Standards	Personal Data Protection Standards 2015.
Third Party	In relation to Personal Data, means any person other than: (a) a Data Subject; (b) a relevant person in relation to a Data Subject; (c) a Data User; (d) a Data Processor; or (e) a person authorized in writing by a Data User to process Personal Data under the direct control of the Data User.
Writing / Written	All manual or electronic methods of recording information in a form capable of being stored and printed, whether in manuscript, using a typewriter or computer, or using other electronic communications devices.

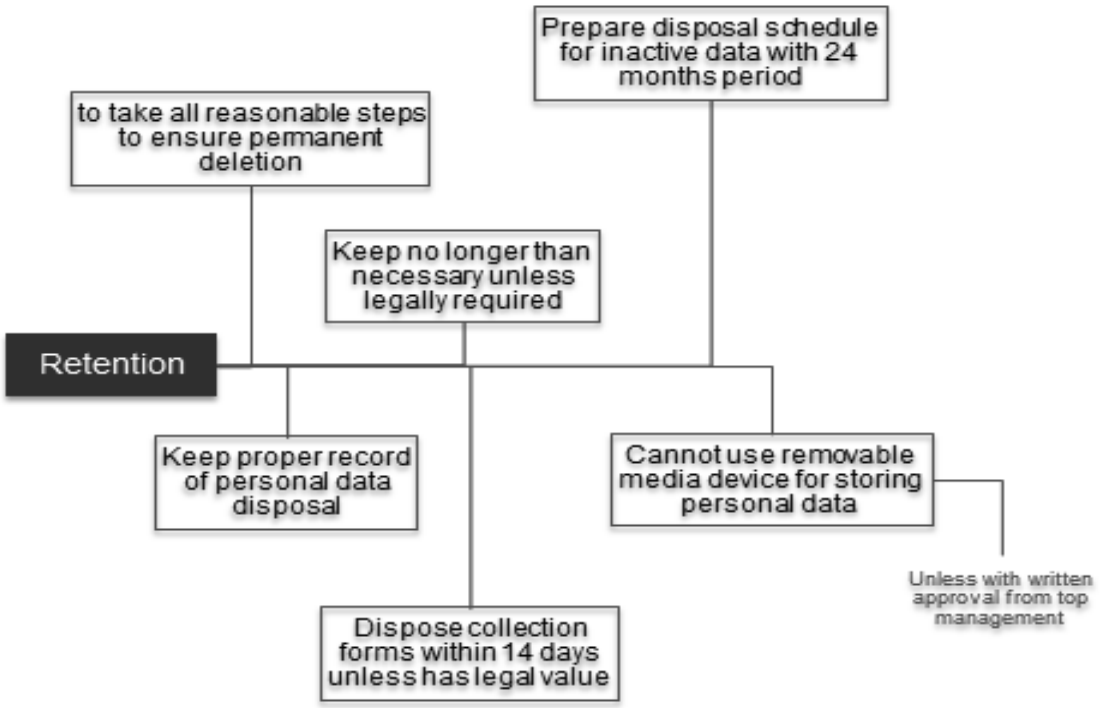
APPENDIX 2: DATA FLOW




for promotion and marketing
to provide services
for legal or regulatory purposes
Why?
for financial purposes
for safety and wellbeing
to investigate complaints and enquiries
to facilitate flight arrangements
Service providers
Affiliates
Disclosed to whom? (third parties)
Overseas Affiliates


Management
Security
Register those allowed access
Control and limit access based on necessity
Cannot transfer via removable device and cloud computing service
Unless with written consent of top management
Maintain proper record of access and transfer
Bind third party involved
Establish physical security procedures
Ensure all employees protect confidentiality


Access/Integrity
Access Request Form
For Personal Data
with a copy
Maximum fee of RM10
without copy
Maximum fee of RM2
For Sensitive Personal Data
with a copy
Maximum fee of RM30
without a copy
Maximum fee of RM 5
Correction Request Form
No fee chargeable
Update personal data immediately upon receipt


Prepare disposal schedule for inactive data with 24 months period
to take all reasonable steps to ensure permanent deletion
Keep no longer than necessary unless legally required
Retention
Keep proper record of personal data disposal
Cannot use removable media device for storing personal data
Unless with written approval from top management
Dispose collection forms within 14 days unless has legal value

APPENDIX 3: GENERAL PRINCIPLE

Template Consent for Online Collection of Personal Data

Template consent language which customer will need to agree to before being able to proceed with a booking.

- ☐ *I have read and understood **[insert airline]** Privacy Policy **[hyperlinked]** and agree to **[insert airline]** using my personal information as described in the said policy, including any disclosures and transfers as necessary.*

Template consent language for direct marketing. Customer must expressly indicate consent to receive direct marketing from the airline.

- ☐ *I'd like to receive future communications and updates from **[insert airline]** and its partners.*

APPENDIX 4: NOTICE AND CHOICE PRINCIPLE

Template Privacy Notice

1. Introduction

[Insert name] (referred to as the "**Company**", "**we**", "**our**" or "**us**") is committed to the protection of your Personal Data and takes the matter of protecting your privacy as high priority.

This Privacy Statement explains general terms on how we collect, use and protect the privacy of your Personal Data under the Personal Data Protection Act 2010 ("**PDPA**").

2. What Personal Data do we collect?

The types of Personal Data that we collect directly from you or from third parties depend on the circumstances of collection and on the nature of the service requested or transaction undertaken. It may include (but is not limited to):

[please delete where not applicable]

(a) personal information that links back to an individual, e.g., name, gender, date of birth, passport, other government issued National Identification card numbers and other personal identification numbers;
(b) contact information, e.g., address, phone number and email address;
(c) payment information, e.g., credit or debit card information, including the name of cardholder, card number, billing address and expiry date;
(d) travel information, e.g., flight information, loyalty program membership details, seating, dietary or other service preferences;
(e) health information, e.g., health issues relevant to your travel arrangement or medical records and requests;
(f) technical information, e.g., IP address; and
(g) statistical data, e.g., number of passengers, and hits to website.

Where another person makes reservations on your behalf, you undertake and will ensure that you have authorized the disclosure of your Personal Data and consent to the terms and conditions of this Privacy Statement. Where you are booking on behalf of another person, you represent and warrant that you have the consent of those persons to provide their Personal Data. In addition where you are booking on behalf of children (those below 18 of age), please ensure that you are over 18, has appropriate authority and consent of their consent whose Personal Data is submitted to the Data User.

3. How do we collect your Personal Data?

This Privacy Policy covers any Personal Data provided to us:

[please delete where not applicable]

(a) when making a booking with us, checking-in for a flight or lodging freight;
(b) via any online sites operated by us and our contractors;
(c) under any other contractual agreement or arrangement;
(d) via a third party, e.g., travel agent or our service provider;

Some of the other ways we may collect Personal data shall include (but is not limited to):

(a) communications with you via telephone, letter, fax and email;
(b) when you visit our website or one of our contractors' websites;
(c) when you contact us in person;
(d) when we contact you in person;
(e) when we collect information about you from third parties;
(f) when you interact with us via social media or interactive applications including but not limited to Facebook, Twitter, Instagram etc;
(g) from publicly available sources;
(h) mobile services; and
(i) other channels including our ticketing counters and airport operations.

4. How do we collect your Personal Data from our website?

From our website, we collect your Personal Data in the following ways:

(a) IP Address

We use your IP address to help diagnose problems with our server, and to administer our website. IP addresses are not linked to personally identifiable information.

(b) Cookies

A cookie is an element of data that a website can send to your browser, which may then store it on your system. We use cookies in some of our pages to store your preferences and record session information. The information that we collect is then used to ensure a more personalized service level

for our users. Please be assured though that your credit card number will not be saved for security reasons. You must type the credit card number each time you make a purchase.

You can adjust settings on your browser so that you will be notified when you receive a cookie. Please refer to your browser documentation to check if cookies have been enabled on your computer or to request not to receive cookies. As cookies allow you to take advantage of some of the Website's essential features, we recommend that you accept cookies. For instance, if you block or otherwise reject our cookies, you will not be able to book flights or use any products or services on the Website that require you to log-in.

It is important that you prevent unauthorised access to your password and your computer. You should always log out after using a shared computer.

We also utilise cookies to track the effectiveness of online advertising. This information is treated confidentially and will not be shared with anyone outside of the Company unless otherwise stated in this Privacy Policy. We will only use this information to make informed decisions with regard to the purchase of online advertising.

(c) Online Reservation System

Our online reservation system resides in a secure server that encrypts your purchase information using Secure Socket Layers. We use all reasonable endeavours to protect Personal Data from loss, misuse and alteration. Only authorized employees and agents will have access to your Personal Data. However, you are responsible for your user ID or password that is used on our web site. You should take due care to protect them.

(d) User Feedback Form

Our Customer Care Feedback Form requires you to give us contact information (e.g. your name and email address) so that we can respond to your comments. We use your contact information from the registration form to send you information about our company. Your contact information is also used to contact you where necessary. Demographic and profile data are also collected at our site. We use your Personal Data to tailor your experience at our site by showing you contents that we think you may be interested in contents according to your preferences.

(e) Site Tracking

We use tracking software to monitor customer traffic patterns and site usage to help us develop the design and layout of the websites. This software does not enable us to capture any personal passenger information.

5. What do we use your Personal Data for?

We may use your Personal Data for the following purposes:

(a) to enable us to provide our services and perform our services to you;
(b) to facilitate your travel (e.g., making a booking) and freight arrangements;
(c) to verify identity of passengers and perform luggage check-ins;
(d) to provide flight alert messages;
(e) to facilitate internet check-in;
(f) to process any commercial transaction (e.g. In-flight sales);
(g) to facilitate your participation in our or third parties' loyalty programs;
(h) to protect the safety and well being of yourself and/or other customers;
(i) to investigate and respond to claims and inquiries from you;
(j) to remind you to complete your booking and/or offer our assistance (in case, for instance, failure to complete due to technical difficulties). This is an optional service. You can choose not to receive these emails at any time by following the link at the bottom of each such email;
(k) to provide in-flight catering and other services that best meet your preferences and needs;
(l) for financial purposes such as credit or other payment card verification, accounting, billing and audit; and / or
(m) for business development purposes such as statistical and marketing analysis, systems testing, maintenance and development, customer surveys, customer relations to advise on alterations to flights or to help us in any future dealings with you, for example by identifying your requirements and preference;
(n) to comply with any legal or regulatory requirements; and/ or
(o) for all other purposes ancillary to any of the purposes stated above.

("**Core Purposes**")

(p) to communicate promotions, offers, product, services and information on products and activities, offers to upgrade or other notifications in relation to your booking;

(q) marketing and communicating with you in relation to products and services offered by us and our service partners as well s our appointed agents; and / or

(r) for all other purposes ancillary to any of the purposes stated above.

("**Ancillary Purposes**")

(collectively, "**Purposes**")

6. Accessing/ Limiting/ Correcting/ Updating your Personal Data

You may request to obtain information of your Personal Data, limit the processing of your Personal Data and also update or make amendments to your Personal Data as below:

(a) for online registered customers, you may login to your online account and update your Personal Data; or

(b) for every other customer, you may forward your request to the contact person as detailed below at clause 12.

Please note that depending on the information requested, a nominal fee may be charged. We will endeavour to provide the information back to you as soon as practicable. However we also reserve the right to validate all requests for the authenticity of the request. We may refuse to comply with data access request in circumstances as provided by the law (under section 32 of the PDPA). If we are not able to comply with your request, we will notify you of the reasons.

7. Withdrawing Consent

Please note that it is obligatory for the Company to process your Personal Data for the Core Purpose as stated above, without which we will not be able to make travel arrangements for you. If we do not have your consent to process your Personal Data for the Ancillary Purposes, we will not be able to keep you updated about our future, new and/or enhanced services and products.

Nevertheless, you may stop receiving promotional activities by:

(a) unsubscribing from the mailing list;

(b) editing the relevant account settings to unsubscribe; or

(c) sending a request to ***[insert email address]***

8. To whom do we disclose your Personal Data?

We will not trade or sell your Personal Data to third parties. Your Personal Data shall only be disclosed or transferred to the following third parties who may be located within or outside Malaysia for the fulfilment of the Purpose:

[please delete where not applicable]

(a) our travel and freight service providers or travel-related businesses;
(b) our partner airlines and other carriers;
(c) airport authorities;
(d) our other affiliates and subsidiaries where it is necessary to facilitate your travel;
(e) credit card verification providers,
(f) data warehouse;
(g) IT service providers;
(h) data analytics and/or marketing agency;
(i) other third parties in order to process your commercial transactions;
(j) legal bodies as permitted or required by law such as in compliance with a warrant or subpoena issued by a court of competent jurisdiction; and/or
(k) customs, immigration or other regulatory authorities applicable to you; and/or
(l) safety and security personnel.

In addition to the above, your personal data may also be disclosed or transferred to any of the Company's actual and potential assignee, transferee or acquirer (within or outside Malaysia) (including our affiliates and subsidiaries) or our business, assets or group companies, or in connection with any corporate restructuring or exercise including the our restructuring to transfer the business, assets and/or liabilities.

We shall take practical steps to ensure that their employees, officers, agents, consultants, contractors and such other third parties mentioned above who are involved in the collection, use and disclosure of your Personal Data will observe and adhere to the terms of this Privacy Statement.

9. How is Personal Data stored?

We will store the Personal Data in the country in which we are based ie Malaysia. However, the Company may have back up and storage servers, which are located overseas. Additionally, the Company will secure the storage in following ways in compliance with the minimum security measures prescribed under the PDPA, its regulation and standards:

(a) register all those who are allowed access;
(b) control and limit access based on necessity;
(c) maintain proper record of access and transfer of Personal Data;
(d) ensure all employees of the Company protect confidentiality;
(e) conduct awareness programmes to all employees (if necessary) on responsibility to protect Personal Data;
(f) establish physical security procedures;
(g) bind third parties involved in processing of Personal Data; and
(h) do not use removable device and cloud computing service to transfer or store Personal Data unless with written consent from top management of the Company.

10. How long may we retain your Personal Data?

We will not retain your Personal Data longer than necessary for the fulfilment of the Purpose. However, relevant Personal Data may be retained subject to the conditions below:

(a) as and when required under legislation; or
(b) where legal actions have arisen and are pending.

The Company shall take all reasonable steps to ensure that all Personal Data is destroyed or permanently deleted when no longer required for the Purpose and prepare disposal schedule for inactive data with 24 month period.

11. Changes to Privacy Statement

Please note that this Privacy Statement may be amended from time to time in accordance to applicable laws and regulations and such variations may be applicable to you.

The latest version of this Privacy Statement will be made available to all customers. Do revisit our website from time to time for updates on our Privacy Statement.

12. Links to third party website

We may link this website and/or our applications to other companies or organizations websites (collectively, "**Third Party Sites**"). This Privacy Notice does not apply to such Third Party Sites as those sites are outside our control. If you access Third Party Sites using the links provided, the operators of these sites may collect your personal information. Please ensure that you are satisfied with the privacy statements of these Third Party Sites before you submit any personal information. We try, as far as we can, to ensure that all third

party linked sites have equivalent measures for protection of your personal information, but we cannot be held responsible legally or otherwise for the activities, privacy policies or levels of privacy compliance of these Third Party Sites.

13. Contact Information

If you still have inquiries or complaints in relation to our handling of your Personal Data or our Privacy Policy or wish to access, update or amend your Personal Data as mentioned above at Clause 6, please visit contact us via the details as described below:

Designation : ***[insert]***

Phone no. : ***[insert]***

Fax no. (if any) : ***[insert]***

Email Address (if any) : ***[insert]***

You may also insert any other related information eg office address

APPENDIX 5: PERSONAL DATA DISCLOSED OR RECEIVED FROM THIRD PARTIES

List of Disclosures

(This Appendix is not intended to be exhaustive but may be amended from time to time as approved by the Personal Data Protection Commissioner)

NO.	THIRD PARTIES
1.	Financial institutions, merchants, VISA International Services Association, MasterCard International Incorporated and other card associations (in relation to credit cards issue to Data Subject) for the purpose of payment of air ticket or other services of the Data User
2.	Postal providers which provide postal services to Data User
3.	Telecommunication providers which provides telecommunication services to the Data User
4.	Service Providers which assist the Data User in processing the services that the Data User requested: (a) Travel and freight service providers or travel-related businesses (b) Partner airlines and other carriers (c) Airport authorities (d) Data User's other affiliates and subsidiaries where necessary to facilitate Data Subject's travel
5.	Agents/ contractors/ consultants/ vendors/ external auditors/ counsellor/ data processor appointed by the Data User (a) Data warehouse (b) IT service providers (c) Data analytics agency (d) Marketing agency
6.	Approved bodies where employees contributions are remitted: (a) Social Security Organisation (SOCSO) (b) Baitulmal (c) Pusat Zakat (d) Lembaga Tabung Haji (e) Yayasan Pembangunan Ekonomi Islam Malaysia (YaPEIM) (f) Employees Provident Fund (EPF) (g) Koperasi Wawasan Pekerja-pekerja Berhad (KOWAJA)

	(h) Insurer/ Broker
7.	Close family member of Data Subject: (a) Father (b) Mother (c) Husband (d) Wife (e) Siblings
8.	Federal Government or State Government requesting information from the Data User. The following are examples stated, as such it is including but not limited to as below: (a) Department of Islamic Development Malaysia (b) Department of Legal Aid Malaysia (c) Department of Statistics Malaysia (d) Immigration Department of Malaysia (e) Inland Revenue Board of Malaysia (matters relating to income tax) (f) Majlis Amanah Rakyat under Ministry of Rural and Regional Department (g) Malaysian Anti-Corruption Commission (h) Malaysia Department of Insolvency (i) Ministry of Domestic Trade, Co-operatives and Consumerism (j) Ministry of Finance Malaysia (k) Ministry of Health (l) Ministry of Human Resources Malaysia (m) Royal Malaysian Customs Department (n) Royal Malaysia Police (o) Security Commission (p) Syariah Judiciary Department Malaysia (q) Jabatan Agama (r) Majlis Perbandaran (s) Majlis Daerah (t) Majlis Agama Islam Negeri

	(u) The National Higher Education Fund Corporation (PTPTN) (v) The National Film Development Corporation Malaysia (FINAS)
9.	Wholly owned subsidiaries of Data User
10.	Panel doctors/ clinics/ hospitals/ pharmacists appointed by Data User
11.	Data User's safety and security personnel
12.	Any person connected to the enforcement or preservation on the Data User's right under the agreements which have been entered with the Data User
13.	Company and organization that assist the Data User in providing value services that the Data Subject requested
14.	Any person notified and authorized by the Data Subject
15.	Any person intending to settle the outstanding amount in relation to the Data User services to the Data Subject
16.	Where Data Users are required or authorized by any court order / tribunal or authority whether government or quasi government with jurisdiction over Data User
17.	Any person/ company appointed by the Data User to recover the outstanding debt of the Data User
18.	Data User advisers (including but not limited to accountants, auditors, lawyers or other professional advisers) as authorized by Data Subject
19.	Parties that Data User required or permitted by law
20.	Parties that the Data User may transfer rights and obligations pursuant to the agreement endorsed with the Data Subject
21.	Data User's actual and potential assignee, transferee or acquirer (within or outside Malaysia) of its business, assets or group companies or in connection with any corporate restructuring or exercise

Personal Data Received From Third Parties

[The third party] shall fully comply with the provisions of the Personal Data Protection Act and any regulations, regulatory guidance, orders, standards, directions, codes of practice or other similar regulatory instrument issued pursuant to it ("**the Act**") applicable to the processing of personal data as defined in the Act and specifically, that all necessary consents have been obtained from individuals whose personal data may be disclosed to Airline pursuant to the Agreement ("**Disclosed Data**") in respect of such disclosure to and processing by Airline and that [*the third party*] will always furnish Airline with up-to-date Disclosed Data.

[The third party] shall indemnify Airline against all proceedings, costs, expenses, liabilities or damages arising from [the third party's] failure to comply with the Act with respect to any Disclosed Data. The remedies available to Airline contained in this clause are without prejudice to and are in addition to any warranties, indemnities, remedy or other rights provided by law or the Agreement.

Personal Data Disclosed to Third Parties

1. Data Processor shall comply with the Personal Data Protection Act and any regulations, regulatory guidance, orders, standards, directions, codes of practice or other similar regulatory instrument issued pursuant to it in respect of the processing of Personal Data (collectively, "**Privacy Laws**").
2. Data Processor shall process personal data only on behalf of and for the benefit of Airline, for the purposes of processing personal data in connection with the Agreement, and to carry out its obligations pursuant to the Agreement and Airline's written instructions.
3. Airline shall have the exclusive authority to determine the purposes for and means of processing personal data under this Agreement.
4. Data Processor and its employees, agents, consultants or contractors ("**Personnel**") shall hold in strict confidence any and all Personal Data.
5. Data Processor shall limit access to personal data to its Personnel who have a need to know the personal data as a condition to Data Processor's performance of services for or on behalf of Airline.
6. Where Data Processor shares, transfers, discloses or otherwise provides access to any personal data to any third party or contracts any of its rights or obligations concerning Personal Data, Data Processor shall enter into a written agreement with each contractor or third party that imposes obligations on the contractor or third party that are substantially similar to those imposed on Data Processor under this Agreement.
7. Data Processor shall only retain contractors that Data Processor can reasonably expect to appropriately protect the privacy, confidentiality and security of the Personal Data.
8. Data Processor shall not transfer personal data outside Malaysia without the explicit written consent of Airline.
9. Data Processor shall respond to any requests with respect to personal data received from Airline's customers, consumers, employees or others in accordance with Airline's instructions. Data Processor shall cooperate with Airline if an individual requests access to his or her personal data for any reason.
10. Data Processor shall notify Airline immediately in writing of any subpoena or other judicial or administrative order by a government authority or proceeding seeking access to or disclosure of personal data. Airline shall have the right to defend such action in lieu of and on behalf of Data Processor. Airline may, if it so chooses, seek a protective order. Data Processor shall reasonably cooperate with Airline in such defense.
11. Data Processor shall maintain reasonable safeguards and other security measures designed to (i) ensure the security and confidentiality of personal data; (ii) protect against any anticipated threats or hazards to the security and integrity of personal data; and (iii) protect against any actual or suspected

unauthorized processing, loss, use, disclosure or acquisition of or access to any personal data ("**Information Security Incident**").

12. Data Processor shall promptly inform Airline in writing of any Information Security Incident of which Data Processor becomes aware, but in no case longer than 24 hours after it becomes aware of the Information Security Incident. Such notice shall summarize in reasonable detail the effect on Airline, if known, of the Information Security Incident and the corrective action taken or to be taken by Data Processor. Data Processor shall promptly take all necessary and advisable corrective actions, and shall cooperate fully with Airline in all reasonable and lawful efforts to prevent, mitigate or rectify such Information Security Incident. The content of any filings, communications, notices, press releases or reports related to any Information Security Incident must be approved by Airline prior to any publication or communication thereof.
13. Promptly upon the expiration or earlier termination of the Agreement, or such earlier time as Airline requests, Data Processor shall return to Airline or its designee, or at Airline's request, securely destroy or render unreadable or undecipherable if return is not reasonably feasible or desirable to Airline (which decision shall be based solely on Airline's written statement), each and every original and copy in every media of all personal data in Data Processor's possession, custody or control. In the event applicable law does not permit Data Processor to comply with the delivery or destruction of the personal data, Data Processor warrants that it shall ensure the confidentiality of the personal data and that it shall not use or disclose any personal data after termination of the Agreement.
14. Airline shall have the right to monitor Data Processor's compliance with the terms of this Agreement. During normal business hours, and without prior notice, Airline or its authorized representatives may inspect Data Processor's facilities and equipment, and any information or materials in Data Processor's possession, custody or control, relating in any way to Data Processor's obligations under this Agreement. An inspection performed pursuant to this Agreement shall not unreasonably interfere with the normal conduct of Data Processor's business. Data Processor shall cooperate fully with any such inspection initiated by Airline.
15. Data Processor shall deal promptly and appropriately with any inquiries from Airline relating to the processing of personal data subject to the Agreement.
16. Data Processor agrees to indemnify and hold harmless Airline and its officers, employees, directors and agents from, and at Airline's option defend against, any and all claims, losses, liabilities, costs and expenses, including third-party claims, reasonable attorneys' fees, consultants' fees and court costs (collectively, "**Claims**"), to the extent that such Claims arise from, or may be in any way attributable to (i) any violation of this Agreement; (ii) the negligence, gross negligence, bad faith, or intentional or willful misconduct of Data Processor or its Personnel in connection with obligations set forth in this

Agreement; (iii) Data Processor's use of any contractor providing services in connection with or relating to Data Processor's performance under this Agreement; or (iv) any Information Security Incident involving personal data in Data Processor's possession, custody or control, or for which Data Processor is otherwise responsible.

APPENDIX 6: DATA ACCESS REQUEST / DATA CORRECTION REQUEST FORM

PERSONAL DATA CORRECTION REQUEST FORM

For the purpose of this form, Data Subject/Relevant Person (as defined under the Personal Data Protection Act 2010) must provide a copy of the identification card (NRIC) or passport, authorisation letter by the Data Subject (where you are requesting on behalf of the Data Subject) and other relevant supporting document as required by us. Please note that, we may not be able to process your request in the event of the personal data provided is inaccurate, incomplete, misleading or not up to date in the first place. A request to correct personal data is subject to the requirements under Personal Data Protection Act 2010.

SECTION 1 : TO BE FILLED IN BY DATA SUBJECT	
Full Name as per NRIC	
New NRIC (Attach copy)	
*House Phone	
*Office Phone	
Mobile Phone	
SECTION 2 : TO BE FILLED IN BY RELEVANT PERSON	
A : Particulars of Data Subject	
Full Name as per NRIC	
New NRIC (Attach copy)	
B : Particulars of Relevant Person	
Full Name as per NRIC	
New NRIC (Attach copy)	
Address	
*House Phone	
*Office Phone	
Mobile Phone	
**Non-mandatory information*	

CORRECTION OF DATA SUBJECT'S PERSONAL DATA

Please provide a description of the personal data to be corrected.

Declaration by the Data Subject	Declaration by the Relevant Person
I,…… …….. hereby certify that the information given in this form and any documents sumitted are true and accurate. Signature:…… Date:…….	I,……... …….. hereby certify that the information given in this form and any documents submitted are true and accurate. I, hereby agreed that you may contact the Data Subject to verify my identity. Signature:…… Date:……

Note: If GST is imposed on the Fee, the Data Subject will pay for all GST.

****

FOR OFFICIAL USE ONLY
[Insert name] approves / rejects (tick as appropriate) this request made on ***[date of request]*** at ***[location of branch]***. Reasons for rejection: ☐ unable to verify identity of the requestor; ☐ unable to verify that the requestor is authorised to act on behalf of the data subject; ☐ unable to verify that the personal data is inaccurate, incomplete, misleading or not up-to-date; ☐ unable to verify that the correction is accurate, complete, not misleading or up-to-date; or

☐ other reasons as permitted as permitted under the Malaysian Personal Data Protection Act:_____

_____

Staff Name: Signature and Date:

_____ _____

PERSONAL DATA ACCESS REQUEST FORM

For the purpose of this form, Data Subject/Relevant Person (as defined under the Personal Data Protection Act 2010) must provide a copy of the identification card (NRIC) or passport, authorisation letter by the Data Subject and other relevant supporting document as required by us. Please note that, we may not be able to process your request in the event of the personal data provided is inaccurate, incomplete, misleading or not up to date in the first place. A request to access personal data is subject to a fee and also to the requirements under Personal Data Protection Act 2010.

SECTION 1 : TO BE FILLED IN BY DATA SUBJECT	
Full Name as per NRIC	
New NRIC (Attach copy)	
*House Phone	
*Office Phone	
Mobile Phone	
SECTION 2 : TO BE FILLED IN BY RELEVANT PERSON	
A : Particulars of Data Subject	
Full Name as per NRIC	
New NRIC (Attach copy)	
B : Particulars of Relevant Person	
Full Name as per NRIC	
New NRIC (Attach copy)	
Address	
*House Phone	
*Office Phone	
Mobile Phone	
**Non-mandatory information*	

ACCESS OF DATA SUBJECT'S PERSONAL DATA

Please provide a description of the personal data to be accessed.

Do you need a copy of the Personal Data? (Please tick (x) in the relevant box below)

☐ Yes

Item	Description	Fee(RM)
☐ (a)	Personal Data	10
☐ (b)	Sensitive Personal Data	30

☐ No

Item	Description	Fee(RM)
☐ (a)	Personal Data	2
☐ (b)	Sensitive Personal Data	5

Declaration by the Data Subject	Declaration by the Relevant Person
I,…… …….. hereby certify that the information given in this form and any documents sumitted are true and accurate. Signature:…… Date:…….	I,……... …… hereby certify that the information given in this form and any documents submitted are true and accurate. I, hereby agreed that you may contact the Data Subject to verify my identity. Signature:…… Date:……

Note: If GST is imposed on the Fee, the Data Subject will pay for all GST.

****

FOR OFFICIAL USE ONLY
[Insert name] approves / rejects (tick as appropriate) this request made on ***[date of request]*** at ***[location of branch]***. Reasons for rejection:

☐ unable to verify identity of the requestor;

☐ unable to verify that the requestor is authorised to act on behalf of the data subject;

☐ not supplied with information as may reasonably require to locate the personal data which the data access request relates;

☐ the burden or expense of providing access is not proportionate to the risks to Data Subject's privacy in relation to the personal data in question; or

☐ other reasons as permitted as permitted under the Malaysian Personal Data Protection Act:_____

_____

Staff Name: Signature and Date:

_____ _____

KOD TATAAMALAN
PERLINDUNGAN DATA PERIBADI

Untuk Sektor Pengangkutan (Penerbangan)

21 November 2017

PESURUHJAYA PERLINDUNGAN DATA PERIBADI

No. Ruj.
CoP_AVN

PADA menjalankan kuasa yang diberikan oleh Seksyen 23(3) Akta Perlindungan Data Peribadi 2010 (Akta 709), saya dengan ini mendaftarkan Tataamalan bagi Golongan Pengguna Data Pengangkutan dan terpakai kepada semua pengguna data di bawah Golongan tersebut berkuatkuasa serta-merta.

Bertarikh pada: 21 November 2017

(KHALIDAH BINTI MOHD DARUS)
Pesuruhjaya Perlindungan Data Peribadi, Malaysia

ISI KANDUNGAN

1.0 Pengenalan kepada APDP dan Kod Tataamalan

1.1 APDP menetapkan tujuh prinsip perlindungan data seperti berikut:

(a) Prinsip Am ("General Principles")

(b) Prinsip Notis dan Pilihan ("Notice & Choice")

(c) Prinsip Penzahiran ("Disclosre Principles")

(d) Prinsip Keselamatan ("Security Principles")

(e) Prinsip Penyimpanan ("Data Storage")

(f) Prinsip Integriti Data ("Data Integrity Principles")

(g) Prinsip Akses ("Acccess to Data Principles")

1.2 Melanggar terma APDP boleh mengakibatkan liabiliti jenayah. Denda di antara RM10,000 dan RM500,000. Hukuman penjara maksimum tiga (3) tahun boleh dikenakan. Liabiliti peribadi juga boleh dikenakan kepada Pengarah, Ketua Pegawai Eksekutif, Ketua Pegawai Operasi, pengurus, setiausaha dan pegawai-pegawai lain yang seumpamanya melainkan jika mereka dapat membuktikan bahawa: (1) kesalahan tersebut dilakukan tanpa pengetahuannya; dan (2) dia telah mengambil semua langkah berjaga-jaga yang munasabah dan menjalankan usaha yang sewajarnya untuk mencegah sebarang kesalahan.

1.3 Prinsip APDP menetapkan tanggungjawab Pengguna Data secara meluas. Bagaimanapun, APDB memperakui bahawa industri yang berlainan mempunyai tataamalan perniagaan yang berbeza. Justeru itu, ia memberi setiap Pengguna Data budi bicara dan fleksibiliti untuk menangani pematuhan dengan memerlukan kod tataamalan yang khusus untuk setiap kelas pengguna data. Bab 2 menerangkan dengan lebih lanjut tentang tujuan, permohonan dan kesan Kod ini.

1.4 Kod ini menggabungkan keperluan yang ditetapkan di dalam APDP, Peraturan dan Standard untuk menjelaskan bagaimana undang-undang perlindungan data ini digunakan untuk pengendalian data peribadi oleh sektor penerbangan dan memberi tataamalan praktikal yang sesuai untuk sektor penerbangan. Di dalam Kod ini, perkataan-perkataan tertentu digunakan. Perkataan ini ditakrifkan dalam **Lampiran 1: Definasi//Glosari.**

Siapakah yang perlu mengguna pakai Kod ini?

1.5 Kod ini diguna pakai oleh pemegang lesen dan / atau pemegang permit di bawah Akta Suruhanjaya Penerbangan Malaysia 2015, termasuk:

(a) Malaysia Airlines Berhad;
(b) AirAsia Berhad;
(c) AirAsia X Berhad;
(d) MASwings Sdn. Bhd.;
(e) Malindo Airways Sdn Bhd;
(f) Berjaya Air Sdn Bhd; dan
(g) FlyFirefly Sdn Bhd.

1.6 Kod ini diguna pakai untuk semua Data Peribadi dan / atau Data Peribadi Sensitif yang dikendalikan oleh Pengguna Data dalam urus niaga komersial.

Bagaimanakah Kod ini boleh Membantu

1.7 Walaupun APDP menetapkan keperluan undang-undang yang luas untuk diikuti apabila memproses Data Peribadi, ia tidak memberi panduan tentang langkah-langkah praktikal yang boleh diambil untuk mematuhi kod ini. Kod ini membantu mengisi jurang tersebut.

1.8 Kod ini membantu Pengguna Data untuk mengenal pasti isu-isu yang perlu dipertimbangkan semasa memproses Data Peribadi. Pengguna Data akan lebih yakin tentang langkah-langkah yang bersesuaian untuk diambil berkenaan dengan Data Peribadi dan memberikan gambaran yang lebih jelas tentang apa yang tidak boleh diterima apabila berurusan dengan Data Peribadi. Manfaat khusus Kod ini termasuk:

(a) meminimumkan risiko melanggar undang-undang dan tindakan penguatkuasaan yang dijalankan oleh Pesuruhjaya;

(b) kepercayaan orang awam yang lebih baik dengan memastikan perlindungan yang sah yang diperlukan dan dipatuhi;

(c) perlindungan yang lebih baik untuk Subjek Data apabila data mereka diproses;

(d) kepercayaan yang lebih besar dan hubungan yang lebih baik dengan individu yang Data Peribadinya sedang diproses;

(e) mengurangkan risiko reputasi yang disebabkan oleh amalan yang tidak sesuai berkenaan dengan memproses Data Peribadi;

(f) pemahaman yang lebih baik tentang apa dan apa yang tidak boleh diterima apabila berurusan dengan Data Peribadi; dan

(g) mengurangkan risiko soalan, aduan dan pertikaian tentang cara Pengguna Data mengendalikan Data Peribadi.

1.9 Kod ini mempunyai kuasa undang-undang dan ianya berkuatkuasa sebaik sahaja didaftarkan oleh Pesuruhjaya dalam Daftar Kod Tataamalan ("**Tarikh Berkuatkuasa**"). Ia mengikat Pengguna Data untuk mematuhi Kod ini dalam tempoh yang akan ditentukan dan diberitahu secara bertulis oleh Pesuruhjaya. Memandangkan Kod ini terikat secara sah, Pengguna Data yang gagal mematuhi Kod ini dianggap telah melakukan kesalahan, dan apabila disabitkan, boleh didenda sehingga RM100,000 atau dipenjarakan tidak lebih dari satu (1) tahun atau kedua-duanya di bawah Seksyen 29 APDP.

1.10 Kod ini akan melengkapi APDP dan segala peraturan, perintah, standard, arahan, panduan atau instrumen pengawalseliaan serupa yang dikeluarkan menurutnya.

1.11 Sekiranya berlaku konflik di antara Kod ini dengan mana-mana standard yang ditetapkan oleh pengawal selia industri penerbangan sebagaimana yang ditetapkan oleh undang-undang, dokumen yang menetapkan standard yang lebih tinggi akan diguna pakai.

1.12 Contoh-contoh yang diterangkan dalam Kod ini bukanlah secara menyeluruh tetapi adalah untuk tujuan ilustrasi.

1.13 Kod ini adalah tafsiran oleh sektor penerbangan tentang apa yang dikehendaki oleh APDP apabila berurusan dengan Data Peribadi. Cadangan yang disediakan dalam Kod ini adalah tataamalan yang praktikal dan Pengguna Data digalakkan untuk menerima pakai tataamalan ini.

2.0 Penggunaan APDP

(A) Latar Belakang

Apakah Data Peribadi?

2.1 Industri penerbangan menghasilkan sejumlah besar data dari data kejuruteraan dan saintifik hingga kepada data pengguna, data penumpang dan data keselamatan. Walau bagaimanapun, tidak semua data adalah Data Peribadi. Bahagian Kod ini memberikan panduan tentang apa yang dianggap atau tidak dianggap sebagai Data Peribadi.

2.2 Perkara berikut boleh dianggap sebagai Data Peribadi:

(a) maklumat peribadi yang boleh dikenal pasti seperti nama, jantina, tarikh lahir, kewarganegaraan, nombor pasport / nombor kad pengenalan dan negara tempat tinggal;

(b) butiran keadaan kesihatan penumpang seperti, sama ada penumpang sedang hamil;

(c) butiran maklumat pembayaran penumpang seperti maklumat pembayaran yang terkandung dalam e-dompet, maklumat akaun prabayar, maklumat kredit atau kad debit;

(d) butiran kecenderungan cara pemakanan individu dan corak perbelanjaan dalam penerbangan, apabila diproses dengan maklumat peribadi yang boleh dikenal pasti;

(e) butiran maklumat penerbangan individu termasuk maklumat nombor penerbangan, tempat duduk, matawang, destinasi penerbangan; dan

(f) butiran maklumat nombor akaun program kesetiaan individu (jika ada).

2.3 Perkara berikut tidak boleh dianggap sebagai Data Peribadi:

(a) maklumat berhubung kait dengan perniagaan, seperti yang dibincangkan di bawah;

(b) pola trafik di tapak (“generally available information”);

(c) data mengenai individu yang telah meninggal dunia;

(d) data berkaitan individu yang telah digabungkan dan / atau tanpa nama dan identiti di dalam cara yang menyebabkan orang tersebut tidak dapat dikenalpasti; dan

(e) data yang diarkibkan dan / atau disokong secara elektronik (“archived documents”).

Apakah Maklumat Perhubungan Perniagaan?

2.4 Maklumat perhubungan perniagaan adalah dirujuk sebagai maklumat yang telah diproses dalam konteks bisnes ke bisnes seperti maklumat pegawai syarikat, penandatangan yang diberi kuasa, pengarah, pemegang saham individu, penjamin individu, vendor keselamatan individu, vendor atau maklumat perhubungan yang utama. APDP tidak mengecualikan maklumat perhubungan perniagaan secara jelas. Walau bagaimanapun, Pesuruhjaya telah mengambil keputusan bahawa berurusan dengan maklumat perhubungan perniagaan adalah berisiko rendah.

2.5 Pengguna Data boleh mendapatkan maklumat perhubungan perniagaan apabila berurusan dengan organisasi atau syarikat semasa menjalankan perniagaan. Dalam keadaan sedemikian, Pengguna Data

berhak untuk menganggap bahawa organisasi atau syarikat diberi kebenaran untuk memberikan maklumat kepada Pengguna Data.

2.6 Pengguna Data tidak perlu mendapatkan persetujuan dari perhubungan perniagaan ini untuk memproses maklumat mereka bagi tujuan transaksi perniagaan di antara Pengguna Data dan organisasi atau syarikat.

2.7 Walau bagaimanapun, jika Pengguna Data menggunakan Data Peribadi perhubungan perniagaan ini untuk tujuan yang tiada kaitan dengan urus niaga perniagaan, seperti menawarkan tawaran penerbangan kepada perhubungan perniagaan dalam kapasiti peribadinya, maka perhubungan perniagaan tersebut akan dianggap sebagai Subjek Data di bawah APDP.

Contoh A: Syarikat penerbangan X memasuki perundingan dengan penyedia makanan dalam penerbangan untuk menyediakan perkhidmatan katering dalam penerbangan baru. Syarikat penerbangan X memperoleh maklumat tentang pengarah-pengarah penyedia makanan dalam penerbangan, penandatangan yang diberi kuasa, orang perhubung utama dan pemegang saham individu. Syarikat Penerbangan X adalah: (i) berhak untuk menganggap bahawa penyedia makanan dalam penerbangan diberi kuasa untuk memberikan maklumat tersebut; dan (ii) tidak dikehendaki mendapatkan kebenaran pengarah, penandatangan yang diberi kuasa, orang perhubung utama atau pemegang saham individu untuk memproses maklumat mereka.

Apakah Data Peribadi Sensitif?

2.8 Data Peribadi Sensitif adalah:

(a) keadaan fizikal penumpang seperti, sama ada penumpang sedang hamil;

(b) keadaan kesihatan fizikal penumpang seperti adakah penumpang tidak sihat sebelum menaiki pesawat atau penumpang memiliki ketidakupayaan;

(c) kepercayaan keagamaan penumpang; dan

(d) Sejarah jenayah penumpang (jika ada).

2.9 Pengguna Data dikehendaki mendapatkan persetujuan yang **jelas** daripada Subjek Data sebelum memproses Data Peribadi Sensitif.

2.10 Jika Pengguna Data tidak memperolehi persetujuan yang jelas atau ia tidak boleh dilaksanakan atau praktikal untuk Pengguna Data untuk berbuat demikian, Data Peribadi Sensitif boleh diproses di mana pemprosesan diperlukan untuk:

Pekerjaan

(a) untuk menjalankan atau melaksanakan apa-apa hak atau tanggungjawab yang diberikan atau dikenakan oleh undang-undang mengenai Pengguna Data berkaitan dengan pekerjaan;

Kepentingan Kritikal

(b) untuk melindungi kepentingan penting Subjek Data atau orang lain, dalam kes di mana:

(i) kebenaran tidak boleh diberikan oleh atau bagi pihak Subjek Data; atau

(ii) Pengguna Data tidak boleh dipertanggungjawabkan untuk mendapatkan kebenaran Subjek Data,

(iii) kebenaran oleh atau bagi pihak Subjek Data telah ditahan secara tidak munasabah;

Tujuan Perubatan

(c) untuk tujuan perubatan dan dilakukan oleh;

(i) pengamal perubatan profesional; atau

(ii) seseorang yang dalam keadaan terpaksa merahsiakan sesuatu yang bersamaan dengan perkara yang akan timbul jika orang itu adalah seorang profesional penjagaan kesihatan;

Prosiding Undang-Undang

(d) untuk tujuan, atau berkaitan dengan prosiding undang-undang;

Nasihat Undang-Undang

(e) untuk tujuan mendapatkan khidmat nasihat undang-undang;

Mempertahankan Hak Undang-Undang

(f) untuk tujuan mewujudkan, menjalankan atau mempertahankan hak undang-undang;

Pentadbiran Keadilan

(g) untuk pentadbiran keadilan;

Fungsi Yang Sah

(h) untuk menjalankan fungi-fungsi yang diberikan kepada mana-mana orang oleh / atau di bawah mana-mana undang-undang bertulis; atau

Maklumat Awam

(i) di mana maklumat yang terkandung di dalam Data Peribadi telah didedahkan kepada awam akibat perbuatan sengaja oleh Subjek Data.

Apakah itu Pemprosesan?

2.11 APDP diguna pakai untuk Data Peribadi dan Data Peribadi Sensitif yang telah "diproses". Istilah "diproses" terpakai untuk pelbagai aktiviti yang komprehensif dan termasuk pengumpulan awal Data Peribadi, penyimpanan dan penggunaannya, akses, pendedahan serta pelupusan akhir.

2.12 **Lampiran 2: Aliran Data** menetapkan bagaimana data peribadi dikumpul dan diproses oleh syarikat penerbangan dan bagaimana data peribadi sepatutnya diuruskan mengikut tujuh prinsip perlindungan data.

2.13 Pemprosesan Data Peribadi atau Data Peribadi Sensitif adalah tertakluk kepada tujuh prinsip perlindungan data seperti yang dibincangkan di bawah.

(B) Prinsip Am (Seksyen 6 APDP)

Apakah Prinsip Am?

2.14 Prinsip Am menyediakan:

(a) Pengguna Data perlu mendapatkan persetujuan sebelum memproses Data Peribadi. Walau bagaimanapun, persetujuan tidak diperlukan dalam semua keadaan;

(b) Kebenaran yang jelas diperlukan untuk memproses Data Peribadi Sensitif. Ini dibincangkan dengan lebih lanjut seperti di bawah; dan

(c) Pengumpulan dan pemprosesan Data Peribadi mestilah lengkap, berkaitan dan tidak berlebihan untuk tujuan di mana Data Peribadi dikumpul dan diproses.

2.15 Persetujuan tidak diperlukan di mana pemprosesan Data Peribadi adalah:

(a) permintaan oleh Subjek Data dengan tujuan untuk membuat kontrak;

Contoh: *Di mana penumpang yang berpotensi hendak menempah penerbangan daripada Pengguna Data, dia mesti membuat kontrak dengan Pengguna Data, yang merupakan perjanjian pengangkutan Pengguna Data, Persetujuan tidak diperlukan untuk mengumpul nama penumpang dan maklumat perhubungan untuk tujuan memasuki kontrak dengan Pengguna Data.*

(b) untuk pelaksanaan kontrak yang mana Subjek Data adalah suatu pihak yang terlibat;

Contoh: *Di mana seorang penumpang telah menempah tiket dan memasuki perjanjian pengangkutan dengan Pengguna Data, persetujuan tidak diperlukan untuk kakitangan Pengguna Data meminta nama penumpang dan nombor pasport untuk tujuan mengesahkan identiti penumpang dan mendaftar masuk penumpang tersebut ke penerbangan.*

(c) untuk mematuhi apa-apa kewajipan undang-undang Pengguna Data, selain daripada tanggungjawab yang dikenakan oleh sesuatu kontrak;

Contoh: *Di mana Pengguna Data dikehendaki menyediakan Data Peribadi penumpangnya kepada jawatankuasa yang ditubuhkan di bawah Akta Suruhanjaya Penerbangan Malaysia 2015 untuk menyiasat aduan pengguna terhadap Pengguna Data.*

(d) untuk melindungi kepentingan Subjek Data;

Contoh: *Di mana Pengguna Data mendedahkan nama dan alamat dalam operasi mencari dan menyelamat sekiranya berlaku insiden pada pesawat.*

(e) untuk pentadbiran keadilan; atau

Contoh: *Di mana Pengguna Data mempunyai tanggungjawab untuk mendedahkan Data Peribadi kepada pegawai yang diberi kuasa secara bertulis di bawah undang-undang untuk tujuan penyiasatan dan pendakwaan.*

(f) untuk menjalankan apa-apa fungsi yang diberikan kepada mana-mana orang di bawah mana-mana undang-undang atau jika perintah daripada mahkamah undang-undang menghendaki pendedahan Data Peribadi.

Contoh: *Di mana syarikat penerbangan menerima perintah mahkamah untuk mendedahkan maklumat penumpang yang menaiki penerbangan tertentu untuk prosiding pendakwaan di mana tempat penumpang mereka adalah relevan untuk mewujudkan kes pendakwa.*

Bagaimanakah untuk mendapatkan Persetujuan Subjek?

2.16 Persetujuan subjek perlu diperolehi sebelum data peribadi dikumpul. Untuk syarikat penerbangan, data peribadi kebiasaannya dikumpul dari beberapa tempat seperti berikut:

(a) kaunter tiket;
(b) pusat panggilan;
(c) agensi pelancongan;
(d) dari dalam talian, melalui laman *web* atau aplikasi mudah-alih; dan
(e) melalui e-mel atau surat (untuk penerbangan sewa khas dan tempahan berkumpulan).

2.17 Jika Data Peribadi Sensitif dikumpul, kebenaran yang jelas mesti diperolehi melalui pelbagai saluran yang telah ditetapkan oleh prosedur operasi standard Pengguna Data;

2.18 Di mana Data Peribadi Sensitif dikumpulkan melalui saluran lain, seperti secara peribadi, melalui rakaman kebenaran yang jelas atau melalui borang pengumpulan data peribadi dalam talian untuk pelbagai tujuan seperti permintaan penumpang untuk perkhidmatan kerusi roda, pemilihan tempat duduk di dalam baris kecemasan disebabkan oleh suatu keadaan kesihatan atau di mana penumpang hamil, Subjek Data dikehendaki menyatakan dengan jelas tentang persetujuannya. Sebagai contoh, Subjek Data mungkin dikehendaki menurunkan tandatangannya sebagai bukti persetujuan atau menanda di kotak persetujuan yang sesuai.

Kaunter Tiket

2.19 Data peribadi dikumpul apabila pelanggan memberikan nama, nombor pengenalan dan butiran hubungan yang lain apabila membeli tiket penerbangan melalui kaunter tiket lapangan terbang atau kaunter tiket di kawasan luar bandar.

2.20 Sebenarnya, persetujuan tidak diperlukan untuk memproses data peribadi di mana pemprosesan adalah diminta oleh Subjek Data untuk tujuan memasuki kontrak. Kontrak di dalam kes ini adalah kontrak pengangkutan di antara syarikat penerbangan dengan Subjek Data. Walau bagaimanapun, jika Data Peribadi Sensitif diperolehi (seperti sama ada penumpang mempunyai keadaan kesihatan tertentu atau hamil), persetujuan bertulis yang jelas mestilah diperolehi dengan menghendaki Subjek Data sama ada menurunkan tandatangannya sebagai bukti persetujuan atau menanda di kotak persetujuan yang sesuai.

Pusat Panggilan

2.21 Data peribadi dikumpul apabila pelanggan memberi nama, nombor pengenalan dan butiran hubungan lain apabila membeli tiket penerbangan melalui telefon di pusat panggilan syarikat penerbangan.

2.22 Sebenarnya kebenaran tidak diperlukan untuk memproses data peribadi di mana pemprosesan diminta oleh Subjek Data untuk tujuan memasuki kontrak. Kontrak di dalam kes ini adalah kontrak pengangkutan di antara syarikat penerbangan demgan Subjek Data. Walau bagaimanapun, jika Data Peribadi Sensitif diperolehi (seperti sama ada penumpang mempunyai keadaan kesihatan tertentu atau hamil), kebenaran lisan yang jelas mestilah diperolehi daripada Subjek Data.

Kaunter Daftar Masuk

2.23 Data Peribadi dikumpul apabila pelanggan memberikan nama mereka, nombor pengenalan dan/atau nombor pasport semasa daftar masuk di kaunter daftar masuk lapangan terbang.

2.24 Sebenarnya, kebenaran tidak diperlukan untuk memproses data peribadi di mana pemprosesan diminta oleh Subjek Data untuk tujuan memasuki kontrak. Kontrak di dalam kes ini adalah kontrak pengangkutan di antara syarikat penerbangan dengan Subjek Data. Walau bagaimanapun, jika Data Peribadi Sensitif diperolehi (seperti sama ada penumpang mempunyai keadaan kesihatan tertentu atau hamil), persetujuan bertulis yang jelas mestilah diperolehi dengan menghendaki Subjek Data sama ada menurunkankan tandatangannya sebagai bukti persetujuan atau menanda di kotak persetujuan yang sesuai.

2.25 Walau bagaimanapun, syarikat penerbangan masih perlu memberikan Notis Privasi kepada pelanggan. Adalah dicadangkan untuk syarikat penerbangan memaparkan Notis Privasi di tempat utama di kaunter tiket dan memberikan salinan Notis Privasi sekiranya diminta.

Agensi Pelancongan

2.26 Data Peribadi penumpang seperti nama dan maklumat perhubungan boleh didedahkan oleh agensi pelancongan kepada syarikat penerbangan. Data Peribadi Sensitif penumpang seperti keadaan kesihatan boleh juga didedahkan oleh agensi pelancongan.

2.27 Dalam hal ini, syarikat penerbangan perlu mendapatkan jaminan yang bersesuaian daripada agensi pelancongan di mana agensi pelancongan mematuhi APDP dalam memperoleh Data Peribadi dan Data Peribadi Sensitif pelanggan.

2.28 Syarikat penerbangan boleh menggunakan contoh fasal yang diberikan dalam **Lampiran 5: Data Peribadi yang Didedahkan atau Diterima daripada Pihak Ketiga.**

Pengumpulan Dalam Talian

2.29 Data Peribadi boleh diambil daripada pelanggan apabila pelanggan membuka akaun keahlian melalui laman *web* syarikat penerbangan. Pelanggan boleh diminta tentang nama, alamat e-mel dan nombor telefon bimbit semasa membuka akaun dalam talian.

2.30 Sebenarnya, kebenaran tidak diperlukan untuk memproses data peribadi di mana pemprosesan data diminta oleh Subjek Data untuk memasuki kontrak. Kontrak di dalam kes ini adalah kontrak pengangkutan di antara syarikat penerbangan dengan Subjek Data jika data peribadi dikumpul hanya untuk tujuan membolehkan pembelian tiket penerbangan.

2.31 Walau bagaimanapun, syarikat penerbangan mungkin boleh menghantar maklumat terkini dan tawaran ataupun mempelawa pelanggan untuk menyertai program kesetiaan. Dalam kes sedemikian, syarikat penerbangan mesti mendapatkan persetujuan daripada pelanggan. **Lampiran 3: Prinsip Am** menyediakan borang templat untuk persetujuan mengumpul Data Peribadi dalam talian. Selanjutnya, jika Data Peribadi Sensitif diberikan oleh pelanggan, kebenaran bertulis yang jelas mestilah diperolehi dengan menghendaki Subjek Data sama ada menurunkan tandatangannya sebagai bukti persetujuan atau menanda di kotak persetujuan yang sesuai.

2.32 Di mana Subjek Data menempah tiket bagi pihak rakan atau ahli keluarga dan memberikan Data Peribadi rakan dan ahli keluarga (berkemungkinan juga kanak-kanak) kepada syarikat penerbangan. Syarikat penerbangan perlu memastikan bahawa jaminan diberikan oleh pelanggan yang berumur lapan belas (18) tahun ke atas dan mempunyai bidang kuasa yang bersesuaian dan persetujuan dari pihak ketiga yang Data Peribadinya dikemukakan kepada Pengguna Data.

Tataamalan

2.33 Syarikat penerbangan perlu mengenal pasti tempat pengumpulan Data Peribadi yang relevan untuk operasi dan memastikan bahawa bahasa dan mekanisma persetujuan yang sesuai tersedia di tempat pengumpulan ini.

(C) Prinsip Notis dan Pilihan (Seksyen 7 APDP)

2.34 Prinsip Notis dan Pilihan menyediakan bahawa Pengguna Data mesti membuat notis bertulis yang tersedia kepada Subjek Data sebelum atau secepat mungkin selepas mengumpul dan memproses Data Peribadi. Kenyataan bertulis ini juga dikenali sebagai Notis Privasi.

2.35 Notis Privasi adalah pernyataan awam yang menggariskan dengan jelas amalan privasi Pengguna Data.

2.36 **Lampiran 4: Prinsip Notis dan Pilihan** menyediakan templat Notis Privasi yang boleh digunakan oleh Pengguna Data.

Bagaimanakah Notis Privasi dikomunikasikan?

2.37 Notis Privasi harus dikomunikasikan di semua tempat di mana Data Peribadi dikumpul. Ia adalah:

Kaunter Tiket

2.38 Adalah dicadangkan bahawa syarikat penerbangan memaparkan Notis Privasi di tempat utama di kaunter tiket dan memberikan salinan Notis Privasi sekiranya diminta.

Pusat Panggilan

2.39 Adalah dicadangkan bahawa pautan hyper ke Notis Privasi dimasukkan ke dalam tiket penerbangan di mana tiket tersebut akan dikeluarkan kepada pelanggan.

Kaunter Daftar Masuk

2.40 Adalah dicadangkan bahawa syarikat penerbangan memaparkan Notis Privasi di tempat utama di kaunter daftar masuk dan memberikan salinan Notis Privasi sekiranya diminta.

Agensi Pelancongan

2.41 Data peribadi penumpang seperti nama dan maklumat perhubungan boleh dizahirkan oleh agensi pelancongan kepada syarikat penerbangan. Data Peribadi Sensitif seperti keadaan kesihatan penumpang juga boleh didedahkan oleh agensi pelancongan.

2.42 Oleh itu, syarikat penerbangan harus mendapatkan jaminan yang bersesuaian daripada agensi pelancongan bahawa agensi pelancongan tersebut mematuhi APDP dalam mendapatkan Data Peribadi dan Data Peribadi Sensitif pelanggan termasuk menyediakan pelanggan salinan Notis Privasi.

2.43 Syarikat penerbangan boleh menggunakan contoh fasal seperti di **Lampiran 5: Data Peribadi yang Didedahkan atau Diterima daripada Pihak Ketiga.**

Pengumpulan Dalam Talian

2.44 Notis Privasi boleh diberikan kepada pelanggan sebelum membuka akaun secara dalam talian atau sebelum pembelian tiket secara dalam talian oleh pelanggan.

2.45 Jika Data Peribadi telah dikumpul sebelum penguatkuasaan APDP, Pengguna Data perlu memberikan Subjek Data Notis Privasi sebelum:

(a) menggunakan Data Peribadi selain daripada tujuan sebenar semasa ia dikumpul; dan

(b) mendedahkan Data Peribadi kepada mana-mana Pihak Ketiga.

Contoh: *Pengguna Data boleh menghantar e-mel kepada Subjek Data memaklumkan kepada mereka tentang Notis Privasi yang telah dikemaskini atau membuat pengumuman di laman web korporat atau aplikasi mudah-alih korporat Pengguna Data.*

2.46 Pengguna Data juga boleh mengkomunikasikan Notis Privasi mereka, dan dianggap telah disampaikan kepada Subjek Data dengan menggunakan salah satu daripada kaedah berikut:-

(a) dengan menghantar Notis Privasi melalui pos ke alamat terakhir Subjek Data; atau

(b) dengan memaparkan secara jelas Notis Privasi di dalam laman *web* korporat Pengguna Data; atau

(c) dengan memaklumkan Subjek Data menerusi pesanan segera tentang alamat laman *web* korporat / pautan ke Notis Privasi dan / atau nombor telefon untuk meminta maklumat lanjut; atau

(d) dengan memasukkan ringkasan Notis Privasi ke dalam komunikasi tetap dengan Subjek Data dengan berserta alamat laman *web* korporat / pautan ke Notis Privasi dan / atau nombor telefon jika Subjek Data ingin meminta maklumat lanjut; atau

(e) dengan memaparkan ringkasan Notis Privasi di tempat perniagaan Pengguna Data dan menyediakan Notis Privasi penuh apabila diminta di kaunter Pengguna Data; atau

(f) dengan memaparkan mesej di skrin kiosk daftar masuk sendiri Pengguna Data dengan alamat laman *web* korporat / pautan ke Notis Privasi, nombor telefon untuk meminta maklumat lanjut dan / atau menyatakan bahawa Notis Privasi boleh diperolehi di pejabat cawangan Pengguna Data; atau

(g) dengan memasukkan suatu pernyataan dalam borang permohonan / pendaftaran yang merujuk kepada Notis Privasi, dan menyediakan pautan ke laman *web* korporat, atau nombor telefon untuk meminta maklumat lanjut; atau

(h) dengan mencetak salinan Notis Privasi dan memberikannya kepada Data Subjek di premis Pengguna Data; atau

(i) apa-apa kaedah lain untuk mengkomunikasikan Notis Privasi sebagaimana yang telah diluluskan oleh Pesuruhjaya atau yang membawa Notis Privasi kepada perhatian Pengguna Data.

Contoh: *Di mana Pengguna Data memberikan ringkasan Notis Privasi bersama-sama dengan pautan ke Notis Privasi di laman web korporatnya di dalam komunikasi e-mel dengan Subjek Data, ini mencukupi untuk membuktikan bahawa Notis Privasi telah dikomunikasikan kepada Subjek Data.*

2.47 Pengguna Data perlu menentukan cara yang paling sesuai untuk mengkomunikasikan Notis Privasi yang mana jika boleh akan sampai kepada seberapa banyak Subjek Data. Adalah disyorkan bahawa Pengguna Data menggunakan pelbagai kaedah komunikasi untuk memastikan bahawa Notis Privasi dikomunikasikan secara meluas.

Contoh: *Sesetengah Subjek Data mungkin tidak celik komputer. Dalam hal ini, syarikat penerbangan tersebut boleh mengkomunikasikan Notis Privasi melalui telefon semasa tempahan tiket dibuat atau dengan memaparkan ringkasan Notis Privasi di kaunter tempahan tiket masuk dan menyediakan salinan Notis Privasi apabila terdapat permintaan.*

2.48 Notis Privasi, apabila dikomunikasikan oleh Pengguna Data kepada Subjek Data, ia dianggap telah dikomunikasikan bagi pihak anak syarikat, syarikat induk, syarikat bersekutu dan syarikat berkaitan Pengguna Data.

2.49 Syarikat induk ("Headquarters") dibenarkan untuk mengeluarkan Notis Privasi untuk Pegguna Data yang juga adalah anak syarikat dalam kumpulan syarikat yang lebih besar.

2.50 Adalah disyorkan bahawa Pengguna Data mengkomunikasikan Notis Privasi kepada semua Subjek Data, sama ada yang sedia ada atau baru, kerana ini akan meminimumkan beban pentadbiran Pengguna Data dalam memastikan pematuhan.

Bilakah Notis Privasi Diterima?

2.51 APDP tidak memerlukan bukti bahawa Notis Privasi diterima dan / atau diterima oleh Subjek Data.

2.52 Notis Privasi akan dianggap sebagai telah dikomunikasi kepada Subjek Data setiap kali Subjek Data menggunakan perkhidmatan / kemudahan Pengguna Data yang menyediakan Notis Privasi melalui kaedah komunikasi yang dinyatakan di atas.

Penyimpanan Rekod

2.53 Pengguna Data dikehendaki menyimpan rekod setelah menyampaikan Notis Privasi kepada Subjek Data. Keperluan ini adalah untuk mengekalkan bukti / rekod bahawa Pengguna Data telah mengkomunikasikan Notis Privasi kepada Subjek Data.

Contoh: *Di mana Notis Privasi dikomunikasikan kepada Subjek Data dengan memaparkan versi ringkas Notis Privasi di tempat perniagaan Pengguna Data dan menyediakan Notis Privasi penuh di kaunter, pengeluaran Notis Privasi yang diringkaskan dan Notis Privasi penuh sudah cukup untuk membuktikan bahawa Notis Privasi telah dikomunikasikan kepada Subjek Data.*

Contoh: *Di mana Notis Privasi dikomunikasikan melalui e-mel kepada Subjek Data, pengeluaran e-mel adalah merujuk kepada Notis Privasi, Notis Privasi itu sendiri dan penyediaan nama Subjek Data yang dihantar oleh e-mel kepada, adalah memadai untuk membuktikan bahawa Notis Privasi telah dikomunikasikan kepada Subjek Data.*

Contoh: *Di mana Notis Privasi dikomunikasikan melalui perkhidmatan pesanan ringkas kepada Subjek Data, pengeluaran pesanan ringkas tersebut merujuk kepada Notis Privasi, Notis Privasi itu sendiri, dan proses untuk mengkomunikasikan pesanan ringkas tersebut kepada Subjek Data, adalah mencukupi untuk membuktikan bahawa Notis Privasi telah dikomunikasikan kepada Subjek Data.*

Tataamalan

2.54 Adalah disyorkan bahawa Pengguna Data mengenal pasti tempat pengumpulan Data Peribadi dan memastikan bahawa Subjek Data menyedari Notis Privasi tersebut ada di tempat pengumpulan ini.

(D) Prinsip Penzahiran(Seksyen 8 APDP)

2.55 "Penzahiran" tidak ditakrifkan dalam APDP. Seorang Pengguna Data boleh dianggap sebagai telah melakukan "Penzahiran" Data Peribadi apabila mereka menzahirkan Data Peribadi kepada Pihak Ketiga.

2.56 Tujuan pengisytiharan oleh Pengguna Data dalam Notis Privasi untuk pengumpulan Data Peribadi adalah penting kerana ia mempengaruhi sama ada persetujuan tambahan perlu diperolehi di bawah Prinsip Penzahiran. Prinsip Penzahiran berkait rapat dengan Prinsip Notis dan Pilihan.

2.57 Pengguna Data hanya boleh mendedahkan Data Peribadi:

(a) selaras dengan Notis Privasi;

(b) selaras dengan semua keperluan berkanun atau kontrak; atau

(c) untuk tujuan yang dibenarkan oleh Subjek Data.

Apakah Penzahiran yang Dibenarkan?

Penzahiran yang dibenarkan menurut Notis Privasi

2.58 Prinsip Pendedahan memperuntukkan bahawa Pengguna Data boleh mendedahkan Data Peribadi kepada Pihak Ketiga di mana:

(a) penzahiran tersebut adalah untuk tujuan yang diisytiharkan pada tempat pengumpulan seperti yang dinyatakan dalam Notis Privasi; atau

Contoh*: Pengguna Data mungkin telah memaklumkan kepada Subjek Data bahawa Data Peribadi mereka boleh dizahirkan kepada pembekal perkhidmatan pihak ketiga seperti dinyatakan dalam Notis Privasi untuk tujuan membolehkan fungsi perniagaan tertentu boleh dijalankan seperti perkongsian Data Peribadi dengan penyedia perkhidmatan teknologi maklumat untuk tujuan perkhidmatan penyelenggaraan teknologi maklumat.*

(b) penzahiran tersebut adalah untuk tujuan yang berkaitan secara langsung dengan maksud yang diisytiharkan dalam Notis Privasi pada tempat pengumpulan; atau

Contoh: *Di mana Pengguna Data telah memaklumkan kepada Subjek Data bahawa Data Peribadi boleh dizahirkan kepada penyedia perkhidmatan teknologi maklumat untuk tujuan perkhidmatan penyelenggaraan teknologi maklumat, sebagai contoh pendedahan kepada*

pelbagai kakitangan penyedia perkhidmatan teknologi maklumat tersebut untuk tujuan perkhidmatan penyelenggaraan teknologi maklumat.

(c) Penzahiran dibuat kepada Pihak Ketiga yang disebut dalam Notis Privasi atau kepada kelas atau kategori Pihak Ketiga sebagaimana dikenal pasti dalam Notis Privasi (sementara masih mematuhi undang-undang, peraturan, standard dan garis panduan yang berkenaan).

***C*ontoh**: *Di mana Pengguna Data telah memaklumkan kepada Subjek Data bahawa Data Peribadi boleh dizahirkan kepada rakan kongsi syarikat penerbangan untuk tujuan memudahkan penerbangan. Kategori Pihak Ketiga yang berkaitan dalam kes ini adalah rakan kongsi syarikat penerbangan.*

Penzahiran yang Dibenarkan di bawah undang-undang

2.59 Data Peribadi mungkin boleh dizahirkan untuk sebarang tujuan atau kepada mana-mana orang yang tidak disebut dalam Notis Privasi di bawah keadaan berikut:

(a) Persetujuan

Subjek Data telah memberikan persetujuan untuk Penzahiran;

(b) Jenayah

Untuk mencegah atau mengesan jenayah, atau untuk tujuan penyiasatan;

Contoh: *Di mana penipuan telah dilakukan terhadap Pengguna Data dan Pengguna Data menzahirkan maklumat tersebut kepada pakar forensik untuk penyiasatan dalaman.*

(c) Undang-Undang / Mahkamah

Dibenarkan oleh mana-mana undang-undang atau perintah mahkamah;

Contoh*: Di mana Pengguna Data perlu menzahirkan maklumat penumpang dan maklumat penerbangan menurut perintah mahkamah untuk penzahiran.*

(d) Pengawalseliaan

Untuk menjalankan fungsi pengawalseliaan;

(e) Hak Perundangan

Pengguna Data secara munasabah mempunyai hak untuk menzahirkan Data Peribadi;

Contoh: *Di mana Pengguna Data dikehendaki untuk menyediakan Data Peribadi penumpangnya kepada jawatankuasa yang ditubuhkan di bawah Akta Suruhanjaya Penerbangan Malaysia 2015 untuk menyiasat aduan pengguna terhadap Pengguna Data.*

(f) Kepercayaan Munasabah ("Reasonable Test")

Pengguna Data secara munasabah percaya bahawa Subjek Data akan memberikan persetujuan;

Contoh: *Di mana Pengguna Data menzahirkan Data Peribadi kepada waris Subjek Data sekiranya berlaku sebarang kecemasan.*

(g) Kepentingan Awam

Penzahiran dibuat diatas kepentingan awam seperti yang ditentukan oleh Menteri;

(h) Cukai

Ia adalah untuk penilaian atau pemungutan apa-apa cukai atau tanggungjawab atau pengenaan lain yang serupa;

(i) Statistik

Ia adalah untuk statistik atau penyelidikan dalam bentuk agregat dengan hasil yang tidak diketahui dan tidak digunakan untuk perkara lain.

Contoh: *Di mana Pengguna Data menjalankan analisis data untuk menganalisa kelakuan pembelian pelanggan, dengan syarat statistik yang dihasilkan adalah tidak diketahui.*

Berurusan dengan Permintaan Penzahiran

2.60 Di mana Data Peribadi dizahirkan untuk pencegahan dan pengesanan jenayah atau untuk penyiasatan, APDP mengecualikan Pengguna Data daripada memberi maklumat kepada Subjek Data berkenaan dengan penzahiran,walaupun Permintaan Akses Data telah difailkan oleh Pengguna Data

2.61 Dalam menangani permintaan untuk penzahiran, Pengguna Data perlu menentukan sama ada:

(a) penzahiran yang dimaksudkan adalah dibenarkan mengikut Notis Privasi; atau

(b) penzahiran yang dimaksudkan adalah dikecualikan di bawah APDP.

2.62 Adalah dicadangkan bahawa Pengguna Data membuat polisi penzahiran yang memberi panduan tentang penzahiran yang dibenarkan dan prosedur yang perlu diikuti apabila berurusan dengan permintaan pihak ketiga untuk penzahiran.

2.63 Jika permintaan untuk penzahiran ditujukan kepada Pengguna Data oleh badan pengawalseliaan atau badan berkanun, atau penzahiran dikehendaki atau dibenarkan atau dibawah sebarang undang-undang atau di atas perintah mahkamah, Pengguna Data mesti:-

(a) memberikan Data Peribadi yang diminta apabila menerima permintaan bertulis merujuk kepada asas undang-undang yang berkaitan tentang permintaan tersebut; dan

(b) di mana bersesuaian, menetapkan syarat berhubung dengan penggunaan Data Peribadi yang dibenarkan dan pulangannya.

2.64 Pengguna Data tidak diwajibkan untuk mengesahkan atau memeriksa Data Peribadi yang diberikan melainkan ia dikehendaki di atas perintah mahkamah.

Berurusan dengan Penzahiran kepada Pemproses Data

2.65 Pengguna Data berkemungkinan besar menzahirkan Data Peribadi kepada Pemproses Data untuk pelbagai tujuan berkenaan dengan perniagaan Pengguna Data. Sebagai contoh, Pengguna Data mungkin berurusan dengan penyedia perkhidmatan teknologi maklumat untuk mengekalkan sistem perkakasan dan / atau perisian teknologi maklumat. Pengguna Data juga mungkin berurusan dengan agensi analisis data dan/atau agensi pemasaran untuk membantu Pengguna Data dalam mengenal pasti peluang untuk pemasaran produk kepada pelanggan Pengguna Data.

2.66 Di mana Pemproses Data terlibat, adalah disyorkan bahawa Pengguna Data memperoleh jaminan dari Pemproses Data berkenaan dengan Data Peribadi yang akan dizahirkan. Jaminan-jaminan ini mungkin termasuk, antara lain:

(a) pemproses Data hanya akan memproses Data Peribadi untuk tujuan yang berkaitan dengan lantikan oleh Pengguna Data, selaras dengan arahan Pengguna Data, dan tiada tujuan lain; dan

(b) pemproses Data akan mematuhi semua undang-undang, pengawalseliaan dan standard industri berkaitan dengan privasi, kerahsiaan atau keselamatan Data Peribadi.

2.67 **Lampiran 5: Data Peribadi yang Dizahirkan atau Diterima daripada Pihak Ketiga** menetapkan beberapa contoh fasal yang mungkin akan dimasukkan ke dalam perjanjian di antara Pengguna Data dengan Pemproses Data di mana Data Peribadi akan dizahirkan kepada Pemproses Data.

Penyimpanan Rekod

2.68 Peraturan-peraturan tersebut menghendaki Pengguna Data untuk mengekalkan senarai penzahiran kepada Pihak Ketiga termasuk Pemproses Data di mana Pihak Ketiga ini tidak termasuk dalam Notis Privasi.

2.69 Contoh Senarai Penzahiran dinyatakan di dalam **Lampiran 5: Data Peribadi yang Dizahirkan atau Diterima daripada Pihak Ketiga.**

Amalan

2.70 Di mana Pengguna Data boleh meramalkan bahawa penzahiran Data Peribadi kepada kelas tertentu Pihak Ketiga mungkin diperlukan (sama ada sebagai perkara rutin atau disebabkan sifat perniagaan syarikat penerbangan), Pihak Ketiga ini harus dikenalpasti atau disebutkan di dalam Notis Privasi. Setakat mana Pihak Ketiga tidak termasuk dalam Notis Privasi dan Pengguna Data ingin menzahirkan Data Peribadi kepada Pihak Ketiga ini, Pengguna Data harus:

(a) mendapatkan persetujuan Subjek Data; dan

(b) merekodkan penzahiran dedahan kepada kelas tertentu Pihak Ketiga.

(E) Prinsip Keselamatan (Seksyen 9 APDP)

2.71 Prinsip Keselamatan memerlukan Pengguna Data untuk meyimpan Data Peribadi dengan selamat. Pengguna Data dikehendaki mengambil langkah praktikal untuk melindungi Data Peribadi daripada sebarang "kehilangan, penyalahgunaan, pengubahsuaian, akses atau penzahiran, pemindahan atau pemusnahan tanpa kebenaran atau tidak sengaja."

2.72 Maksud "langkah praktikal" akan berbeza dari kes ke kes, bergantung kepada sifat Data Peribadi yang diproses oleh Pengguna Data dan tahap kepekaan yang berhubung kait kepada Data Peribadi atau membahayakan di mana Subjek Data mungkin mengalami kehilangan, penyalahgunaan, pengubahsuaian, akses atau penzahiran, pemindahan atau pemusnahan tanpa kebenaran atau tidak sengaja.

2.73 Pengguna Data harus mengambil langkah-langkah praktikal dalam melaksanakan langkah-langkah keselamatan bagi melindungi Data Peribadi yang di dalam kawalan Pengguna Data, dengan mempertimbangkan perkara berikut:-

(a) sifat Data Peribadi dan bahaya yang akan mengakibatkan kerugian, penyalahgunaan, pengubahsuaian, akses atau penzahiran, pemindahan atau pemusnahan tanpa kebenaran atau tidak sengaja;

(b) tempat atau lokasi di mana Data Peribadi disimpan tidak terdedah kepada ancaman fizikal dan semula jadi;

(c) sebarang langkah-langkah keselamatan yang dimasukkan ke dalam mana-mana peralatan di mana Data Peribadi disimpan;

(d) langkah-langkah yang diambil untuk memastikan kebolehpercayaan, integriti dan kecekapan kakitangan yang mempunyai akses kepada Data Peribadi;dan

(e) langkah-langkah yang diambil untuk memastikan pemindahan Data Peribadi yang selamat.

Contoh: *Jika Pengguna Data mempunyai kakitangan yang bekerja dari rumah, langkah penyulitan maklumat yang bersesuaian dan protokol pengendalian dokumen perlu disediakan bagi memastikan ia tidak menjejaskan keselamatan.*

2.74 Pengguna Data perlu menilai polisi yang sedia ada dan melaksanakan langkah-langkah, termasuk tetapi tidak dihadkan seperti berikut:

<u>Pentadbiran</u>

(a) Perjanjian kerahsiaan / Tiada Penzahiran;

(b) Penyeliaan / pemantauan kakitangan;

(c) Pelan latihan dan pendidikan untuk kakitangan;

(d) Menyimpan rekod kakitangan yang memproses Data;

(e) Menetapkan had kuasa untuk setiap aktiviti memproses Data Peribadi. Akses ke pelbagai Data Peribadi harus dihadkan kepada kakitangan yang diberi kebenaran dengan mengadakan nama pengguna dan kata laluan; dan

(f) Membatalkan hak akses kakitangan Data Peribadi apabila kakitangan tersebut tidak lagi menguruskan Data Peribadi atau tidak lagi bekerja untuk organisasi. Untuk cara elektronik, nama pengguna dan kata laluan harus dibatalkan.

Keselamatan Fizikal

(g) sistem kawalan akses pintu untuk masuk dan keluar daripada premis di mana Data Peribadi disimpan;

(h) menyimpan Data Peribadi di tempat sesuai yang selamat daripada ancaman fizikal dan semula jadi dan tidak terdedah;

(i) menyediakan kamera keselamatan litar tertutup (jika perlu),

(j) menyediakan kawalan keselamatan 24 jam (jika perlu);

(k) untuk Data Peribadi yang diproses secara manual, langkah-langkah keselamatan termasuk:-

(i) memastikan Data Peribadi disimpan di dalam fail dalam keadaan yang teratur;

(ii) memastikan semua fail yang mengandungi Data Peribadi disimpan di dalam tempat yang berkunci;

(iii) memastikan semua kunci disimpan di tempat yang selamat;

(iv) mengekalkan rekod di mana kunci-kunci disimpan; dan

(v) menyimpan Data Peribadi di tempat yang sesuai, di mana Data Peribadi adalah selamat dari ancaman fizikal dan semula jadi dan tidak terdedah.

Contoh: *Sebagai sebahagian daripada amalan keselamatan, syarikat penerbangan perlu memastikan bahawa maklumat di dalam komputer riba dan alat telefon mudah-alih yang diberikan kepada kakitangan adalah disulitkan. Terdapat satu protokol untuk menangani peranti yang telah dicuri termasuk memberitahu perkhidmatan teknologi maklumat dengan segera dan membolehkan maklumat dipadam dari jarak jauh.*

Skrin komputer di pejabat diletakkan dalam keaadan terlindung agar tidak dapat dilihat oleh pelawat. Terdapat sistem untuk pelupusan kertas di mana bahan buangan kertas dikumpulkan di dalam tong dengan selamat dan dicarik di tapak yang sama pada akhir setiap minggu.

Keselamatan teknikal

(l) penyulitan maklumat (*encryption)*;

(m) perisian anti-virus;

(n) polisi teknologi maklumat yang penting seperti tidak membuka lampiran e-mel daripada sumber yang tidak dijangka atau tidak diketahui;

(o) tembok api (*firewalls)*;

(p) menampal perisian. Menampal perisian adalah pembaharuan terkini daripada pencipta perisian sistem operasi atau aplikasi perisian yang biasanya mengandungi penambahbaikan potensi keselamatan;

(q) protokol ketat tentang akses jarak jauh (seperti keupayaan pekerja untuk mengakses rangkaian dari lokasi terpencil). Akses harus dihadkan kepada alamat IP yang khusus;

(r) memastikan keselamatan yang mencukupi di tempat kakitangan yang mengakses pelayar (*server)* syarikat melalui rangkaian tanpa wayar. Pengguna Data harus memastikan bahawa langkah-langkah penyulitan, tembok api, dan sesi-sesi *web* yang selamat disediakan untuk melindungi serangan mesin pihak ketiga apabila menggunakan rangkaian tanpa wayar yang tidak selamat;

(s) komputer riba mudah-alih, kekunci USB, telefon pintar dan lain-lain bentuk peranti mudah-alih harus disulitkan dan kemudahan pemadam memori jauh diaktifkan;

(t) log dan jejak audit (*audit trails*) untuk mengenal pasti penyalahgunaan. Kakitangan perlu dimaklumkan bahawa jejak berkenaan sudah tersedia ada;

(u) sistem sandaran. Pengguna Data harus menentukan kekerapan yang sesuai dan sifat sandaran.

<u>Keselamatan Organisasi</u>

(v) pelan tindak balas insiden. Pengguna Data harus menjangkakan apa yang perlu dilakukan jika terdapat pencerobohan data dan bersedia untuk bertindak balas.

Contoh: *Beberapa isu yang boleh ditangani oleh syarikat penerbangan:*

- *Apakah yang organisasi akan lakukan sekiranya berlaku insiden pencerobohan data?*
- *Adakah terdapat polisi yang menyatakan apakah pencerobohan data? (Ia mungkin termasuk hilang kawalan ke atas data peribadi termasuk akses yang tidak sesuai ke atas sistem organisasi atau penghantaran Data Peribadi kepada pihak yang salah)*

- *Bagaimana anda tahu jika organisasi telah mengalami pencerobohan data? Adakah kakitangan-kakitangan di semua peringkat faham akan implikasi kehilangan Data Peribadi?*
- *Sudahkah organisai anda mengenal pasti kepada siapakah kakitangan-kakitangan perlu laporkan jika mereka kehilangan kawalan ke atas Data Peribadi?*
- *Adakah polisi anda jelas menyatakan siapakah yang bertanggungjawab untuk mengendalikan insiden tersebut?*

2.75 Pengguna Data harus mengkaji secara berkala amalan keselamatannya untuk mengesan kelemahan di dalam organisasi dan menjangka kemungkinan pencerobohan keselamatan. Rekod polisi, semakan dan latihan Pengguna Data harus disimpan.

2.76 Berhubung dengan pemindahan Data Peribadi, Pengguna Data perlu:

(a) memastikan bahawa ia telah memperolehi persetujuan bertulis daripada pengurusan tertinggi untuk pemindahan Data Peribadi menggunakan:-

(i) peranti media mudah-alih (seperti peranti penyimpanan luaran mudah-alih); atau

(ii) perkhidmatan pengkomputeran awan.

(b) merekod semua pemindahan Data Peribadi menggunakan peranti media mudah-alih dan/atau perkhidmatan pengkomputeran awan.

(c) memastikan bahawa pemindahan Data Peribadi dengan cara konvensional seperti melalui pos, dengan tangan, faks dan sebagainya direkodkan.

Berurusan dengan Penzahiran kepada Pemproses Data

2.77 Pengguna Data juga harus memastikan bahawa ia telah menandatangani kontrak dengan Pemproses Data untuk melindungi Data Peribadi daripada kehilangan, penyalahgunaan, pengubahsuaian, akses dan penzahiran tanpa kebenaran. **Lampiran 5: Data Peribadi yang Dizahirkan atau Diterima daripada Pihak Ketiga** menetapkan beberapa contoh fasal yang mungkin akan dimasukkan ke dalam perjanjian di antara Pengguna Data dengan Pemproses Data di mana Data Peribadi dizahirkan kepada Pemproses Data.Ini termasuk:-

(a) kerahsiaan, tiada penzahiran dan keperluan keselamatan;

(b) syarat-syarat Data Peribadi boleh diproses;

(c) perwakilan, akujanji, jaminan dan / atau indemniti yang akan disediakan oleh Pemproses Data; dan

(d) langkah-langkah keselamatan yang mentadbir urus pemprosesan yang akan dijalankan seperti yang terkandung di dalam polisi dan standard keselamatan dalaman Pengguna Data.

Tataamalan

2.78 Pengguna Data dikehendaki untuk melakukan dan melaksanakan polisi keselamatan mengikut Peraturan yang ditetapkan.

(F) Prinsip Penyimpanan (Seksyen 10 APDP)

2.79 Di bawah prinsip penyimpanan, Pengguna Data hanya boleh menyimpan Data Peribadi selama yang diperlukan untuk memenuhi tujuan pemprosesan. Setelah tujuan tersebut dipenuhi, Pengguna Data dikehendaki memusnahkan atau memadamkan semua versi manual dan elektronik Data Peribadi secara kekal.

Bagaimana untuk Mematuhi Prinsip Penyimpanan?

2.80 Beberapa langkah yang boleh diambil oleh Pengguna Data untuk mematuhi Prinsip Penyimpanan termasuk tetapi tidak terhad kepada yang berikut:-

(a) mengenal pasti semua undang-undang yang berkaitan dengan pemprosesan dan penyimpanan Data Peribadi sebelum memusnahkan sebarang Data Peribadi.

(b) Data Peribadi tidak harus disimpan lebih lama daripada yang diperlukan untuk apa-apa tujuan melainkan terdapat peruntukan undang-undang yang memerlukan penyimpanan Data Peribadi yang lebih lama.

APDP tidak mengatasi peruntukan undang-undang lain yang memerlukan penyimpanan maklumat atau dokumen untuk jangka waktu tertentu. Contohnya, Akta Syarikat 1965, Akta Cukai Pendapatan 1967, Akta Pekerjaan 1955, Ordinan Buruh Sabah, Ordinan Buruh Sarawak, Akta Pembatasan 1953, Ordinan Batasan Sarawak dan Ordinan Batasan Sabah (Cap 72) memerlukan dokumen disimpan untuk satu tempoh masa. APDP dan undang-undang lain yang berkenaan mesti dibaca bersama;

(c) Pengguna Data mesti melupuskan borang pengumpulan Data Peribadi yang digunakan untuk tujuan komersial dalam tempoh 14 hari, melainkan borang tersebut mempunyai nilai undang-undang yang dilampirkan pada transaksi komersial.

Pengguna Data mesti memadamkan borang pengumpulan Data Peribadi dalam tempoh empat belas (14) hari penggunaan, melainkan Pengguna Data boleh menunjuk sebab keperluan untuk menyimpan borang tersebut. Sebagai contoh, borang pengumpulan mungkin diperlukan untuk tujuan transaksi yang belum selesai.

(d) Pengguna Data tidak harus menggunakan peranti media mudah-alih untuk menyimpan Data Peribadi tanpa persetujuan bertulis daripada pengurusan atasan.

Pengguna Data harus melarang penggunaan pemacu pen atau "hard disk" luaran tanpa kebenaran bertulis daripada kakitangan yang diberi kuasa.

(e) Pengguna Data mesti menyemak dan memadam Data Peribadi yang tidak lagi diperlukan dari pangkalan data.

(f) Pengguna Data mesti menggunakan jadual pelupusan Data Peribadi untuk melupuskan Data Peribadi yang telah tidak aktif untuk tempoh dua puluh empat (24) bulan. Pengguna Data mesti merekod jadual pelupusan ini.

Pengguna Data harus melaksanakan jadual penyemakan dan pelupusan Data Peribadi secara berkala dan merekodkan prosedur penyemakan dan pelupusan.

(g) Pengguna Data harus mengekalkan rekod tentang pelupusan Data Peribadi yang perlu dikemukakan sebagaimana yang diarahkan oleh Pesuruhjaya.

Berapa Lama Data Peribadi Boleh Disimpan?

2.81 APDP tidak menetapkan tempoh yang membolehkan Data Peribadi disimpan. Oleh itu, ia adalah tertakluk kepada Pengguna Data menyimpan Data Peribadi seperti yang dikehendaki dibawah undang-undang berkanun dan/atau mengikut polisi syarikat.

2.82 Data Peribadi boleh disimpan secara kekal jika ia diperlukan untuk:

(a) prosiding undang-undang atau pengawalseliaan atau penyiasatan yang serupa atau tanggungjawab untuk mengeluarkan maklumat berkenaan;

(b) jenayah disyaki atau dikesan; atau

(c) maklumat yang berpotensi mempunya kepentingan sejarah.

Keperluan ini terpakai untuk salinan dokumen manual dan elektronik yang mengandungi Data Peribadi.

Pemusnahan / Pemadaman Data Peribadi

2.83 Pengguna Data dikehendaki untuk memusnahkan Data Peribadi secara kekal dalam bentuk fizikal dan eletronik.

Contoh: *Seorang kakitangan boleh memusnahkan secara kekal salinan fizikal Data Peribadi dengan mencarik salinan kertas. Data Peribadi versi elektronik boleh dimusnahkan secara kekal dengan menggunakan perisian pemusnah yang selamat, atau mengubah penetapan alat mudah-alih kepada penetapan kilang.*

2.84 Di mana Pengguna Data perlu menyimpan Data Peribadi melebihi tempoh khusus perundangan, ia harus membuktikan keperluan yang munasabah untuknya.

Contoh: *Permulaan prosiding undang-undang atau penyiasatan berkaitan Data Subjek adalah sah untuk terus menyimpan Data Peribadi sehingga pelupusan / penutupan kes tersebut.*

2.85 Sebagai alternatif daripada memusnahkan atau memadamkan Data Peribadi secara kekal, Pengguna Data boleh menjadikan Data Peribadi tersebut tidak mempunyai nama atau identiti ("anonymise"). Data Peribadi tanpa nama dan identiti tidak dianggap sebagai Data Peribadi di bawah APDP kerana ia tidak boleh dikaitkan dengan mana-mana Subjek Data.

Contoh: *Pengguna Data boleh memadamkan maklumat seperti nama, alamat e-mel, nombor telefon, alamat rumah atau pasport dan nombor kad pengenalan.*

Tataamalan

2.86 Untuk melaksanakan tataamalan penyimpanan yang baik, Pengguna Data harus membangunkan standard prosedur operasi untuk tataamalan penyimpanan dan pelupusan Data Peribadi. Kakitangan yang terlibat mesti dilatih untuk melaksanakan prosedur tersebut.

(G) Prinsip Data Integriti (Seksyen 11 APDP)

2.87 Prinsip Data Integriti memerlukan Pengguna Data untuk mengambil langkah-langkah yang munasabah untuk memastikan Data Peribadi adalah tepat, lengkap, tidak mengelirukan dan terkini.

(a) dengan mengambil kira tujuan untuk mengumpul dan memproses Data Peribadi;

(b) mana-mana tujuan yang berkaitan secara langsung.

2.88 Pengguna Data mesti mengambil langkah-langkah yang munasabah untuk memastikan Data Peribadi adalah:

(a) tepat iaitu Data Peribadi diambil dengan betul;

(b) lengkap iaitu butir-butir Data Peribadi tidak tertinggal. Maklumat yang direkodkan oleh Pengguna Data mesti mencerminkan secara tepat maklumat yang diberikan oleh Subjek Data;

(c) tidak mengelirukan iaitu Data Peribadi tidak jelas, palsu atau terdapat kesilapan yang tidak disengajakan. Sebagai contoh, status perkahwinan Subjek Data tidak boleh digambarkan dengan salah oleh Pengguna Data;.

(d) terkini iaitu Pengguna Data harus memastikan bahawa Data Peribadi yang diberikan oleh Subjek Data adalah yang terkini. Sebagai contoh, penukaran alamat yang dibuat oleh Subjek Data mesti direkodkan oleh Pengguna Data.

Apakah Langkah-langkah Munasabah ("Reasonable Steps")?

2.89 Pengguna Data boleh mengambil "langkah-langkah munasabah" untuk mematuhi Prinsip Integriti Data termasuk tetapi tidak terhad kepada:-

(a) menyediakan borang di mana Subjek Data boleh melengkapkan Data Peribadi untuk mengemas kini Data Peribadi sama ada melalui elektronik atau borang fizikal;

(b) mengemas kini Data Peribadi secara serta-merta selepas menerima Permohonan Pembetulan Data daripada Subjek Data;

(c) memastikan undang-undang yang berkaitan dipatuhi dalam menentukan jenis dokumen sokongan yang diperlukan untuk menentukan kesahihan Data Peribadi Subjek Data;

(d) memaklumkan Subjek Data tentang keupayaan mereka untuk mengemas kini Data Peribadi melalui portal atau memaparkan notis di premis Pengguna Data atau cara lain yang bersesuaian;

(e) langkah-langkah munasabah yang lain mengikut tujuan mengapa Data Peribadi dikumpul.

***Contoh**: Di mana Data Peribadi disimpan oleh Pengguna Data untuk tujuan menyediakan maklumat penerbangan yang dibeli oleh Subjek Data, membuat promosi, mengemas kini maklumat terkini atau menaik taraf kepada Subjek Data, adalah munasabah untuk Pengguna Data memastikan bahawa Data Peribadi sentiasa betul dengan cara pengesahan Data Peribadi berdasarkan dokumen pengenalan*

rasmi dari Subjek Data. Walau bagaimanapun, tidak munasabah untuk mengharapkan Pengguna Data memastikan bahawa alamat Subjek Data sentiasa terkini.

***Contoh**: Pengguna Data boleh mengingatkan Subjek Data untuk mengemas kini Data Peribadi dengan memberitahu Subjek Data melalui e-mel dan / atau pada laman web korporat Pengguna Data. Tetapi adalah menjadi tanggungjawab Subjek Data untuk memaklumkan kepada Pengguna Data tentang sebarang perubahan kepada Data Peribadi.*

2.90 Berikut adalah langkah-langkah yang boleh dipertimbangkan oleh Pengguna Data untuk mematuhi Prinsip Integriti Data.

(a) Pengguna Data mungkin memerlukan Subjek Data untuk memaklumkan kepada Pengguna Data sebarang pertukaran kepada Data Peribadinya. Ini adalah supaya Pengguna Data tidak melanggar Prinsip Integriti Data jika Pengguna Data tidak dimaklumkan oleh Subjek Data tentang pertukaran Data Peribadinya.

(b) Pengguna Data harus membolehkan Subjek Data untuk menghantar Permintaan Pembetulan Data untuk mengemas kini atau membetulkan Data Peribadinya di cawangan dan / atau laman *web* korporat Pengguna Data dan di tempat lain yang ada hubungan dengan Subjek Data.

2.91 Pengguna Data tidak akan melanggar Prinsip Data Integriti jika Data Peribadi yang diberikan oleh Subjek Data adalah tidak tepat, tidak lengkap, mengelirukan dan tidak terkini.

2.92 Pengguna Data tidak perlu mengemas kini atau membetulkan Data Peribadi Subjek Data berdasarkan maklumat yang diberikan oleh mana-mana pihak selain Subjek Data.

2.93 Prinsip Data Integriti tidak akan dilanggar jika:-

(a) Pengguna Data menyimpan Data Peribadi yang bersifat bersejarah (sebagai contoh, alamat rumah sebelum atau nombor perhubungan Subjek Data); dan

(b) Pengguna Data menyimpan Data Peribadi yang merekodkan situasi yang berlaku secara kesilapan (sebagai contoh, di mana akaun Subjek Data telah ditamatkan secara tidak sengaja tetapi telah diaktifkan semula, Pengguna Data dibenarkan untuk menyimpan segala rekod kerana ia mencerminkan ralat dengan tepat).

Hak untuk Membetulkan Data Peribadi (Seksyen 34 of APDP)

2.94 Subjek Data berhak untuk memohon supaya Data Peribadi yang dipegang oleh Pengguna Data diperbetulkan di mana mereka menganggap bahawa Data Peribadi tersebut tidak tepat, tidak lengkap, mengelirukan dan tidak terkini.

Pengecualian

2.95 Pengguna Data tidak dikehendaki untuk mematuhi Permintaan Pembetulan Data (PPD) di mana Data Peribadi diproses:

(a) untuk pencegahan atau pengesanan jenayah atau untuk tujuan penyiasatan;

(b) untuk penangkapan atau pendakwaan pesalah;

(c) untuk penilaian atau pungutan cukai atau duti atau pengenaan lain yang serupa;

(d) untuk penyedian statistik atau menjalankan penyelidikan, dengan syarat Data Peribadi tidak diproses untuk tujuan yang lain dan keputusan statistik atau keputusan penyelidikan tidak disebutkan;

(e) untuk tujuan atau berhubung dengan sebarang perintah atau penghakiman mahkamah; atau

(f) untuk tujuan melaksanakan fungsi pengawalseliaan.

Bagaimanakah PPD Berfungsi?

2.96 Subjek Data membuat PPD secara bertulis kepada Pengguna Data.

2.97 Selepas menerima PPD, Pengguna Data mesti mengakui penerimaan permintaan tersebut.

2.98 Selepas membuat pengakuan penerimaan dan mengesahkan bahawa PPD telah lengkap, Pengguna Data mesti melakukan pembetulan yang diperlukan kepada Data Peribadi dan memberikan salinan Data Peribadi yang telah diperbetulkan kepada peminta dalam tempoh masa dua puluh satu (21) hari selepas penerimaan PPD.

2.99 Pengguna Data kemudiannya mengambil langkah-langkah yang munasabah untuk membekalkan Pihak Ketiga perkara yang berkaitan dengan Data Peribadi yang terkini dengan notis bertulis tentang sebab pembetulan dilakukan.

2.100 Selepas tempoh dua puluh satu (21) hari berlalu dan Pengguna Data tidak mematuhi tempoh tersebut, Pengguna Data:

(a) mesti memberitahu Subjek Data secara bertulis sebab kelewatan dan tempoh lanjutan tidak lebih daripada empat belas (14) hari akan diberikan secara automatik kepada Pengguna Data; atau

(b) mesti memberitahu Subjek Data jika ia mempunyai sebab untuk tidak mematuhi PPD.

2.101 Jika 2.100(a) terpakai, Pengguna Data mesti mematuhi PPD dalam masa empat belas (14) hari tempoh lanjutan.

Apakan Syarat untuk PPD yang Sah?

2.102 APDP tidak memberi format yang khusus untuk PPD, Walau bagaimanapun ia mesti:

(a) secara bertulis;

(b) disertakan dengan bayaran seperti yang ditetapkan dibawah Undang-Undang Yuran melainkan dikecualikan oleh Pengguna Data;

(c) mengandungi maklumat yang diperlukan untuk mengkehendaki Pengguna Data untuk mencari Data Peribadi. Sebagai contoh, Subjek Data boleh memberikan maklumat tentang nama, nombor kad pengenalan atau pasport, alamat, nombor akaun;

(d) mengkhususkan Data Peribadi yang perlu diperbetulkan;

(e) di mana permintaan dibuat bagi pihak Subjek Data, dokumen yang diperakui perlu dikemukakan untuk menetapkan hak Subjek Data untuk membuat permintaan.

2.103 Sekiranya mana-mana syarat ini tidak dipenuhi, Pengguna Data hendaklah mengembalikan PPD kepada Subjek Data dan meminta keperluan yang ditinggalkan untuk dihantar semula.

Bagaimana jika saya menerima permintaan secara lisan?

2.104 Pengguna Data tidak perlu untuk membalas permintaan secara lisan. Walau bagaimanapun, Pengguna Data boleh memilih untuk memberi panduan kepada Subjek Data tentang cara yang betul untuk membuat PPD.

Bolehkah orang lain membuat PPD bagi pihak Subjek Data?

2.105 PPD boleh dibuat bagi pihak Subjek Data. Khususnya:

(a) di mana Subjek Data berumur di bawah 18 tahun, ibu bapa, penjaga atau orang yang dipertanggungjawabkan sebagai penjaga untuk Subjek Data boleh membuat PPD;

(b) di mana Subjek Data tidak mampu menguruskan hal ehwal sendiri, seseorang yang dilantik oleh mahkamah untuk menguruskan hal ehwal Subjek Data atau seseorang yang diberi kuasa secara bertulis oleh Subjek Data boleh membuat PPD; atau

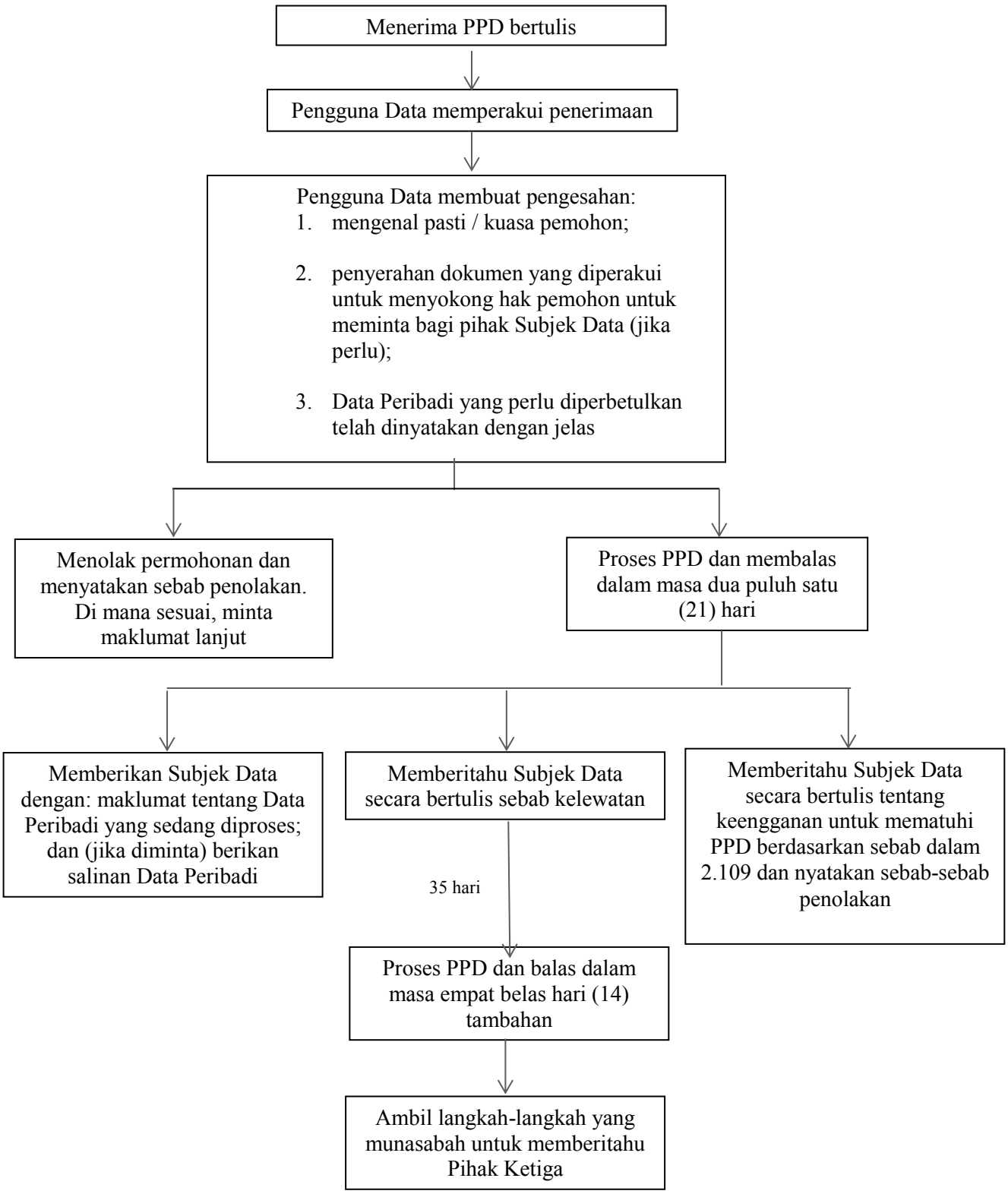
(c) dalam kes yang berlainan, seseorang yang diberi kuasa secara bertulis oleh Subjek Data boleh membuat PPD bagi pihak Subjek Data.

Bagaimana pula dengan Data Peribadi yang dipegang oleh Pihak Ketiga?

2.106 Di mana Data Peribadi telah dizahirkan kepada Pihak Ketiga dalam masa dua belas (12) bulan sebelum hari PPD diterima, dan Pihak Ketiga belum lagi berhenti menggunakan Data Peribadi, Pengguna Data mesti mengambil langkah-langkah yang munasabah dengan memberikan salinan Data Peribadi yang terkini kepada Pihak Ketiga.

Apakah Prosedur untuk Memproses PPD?

2.107 Carta di bawah menunjukkan langkah-langkah yang perlu diambil oleh Pengguna Data setelah menerima PPD.


Menerima PPD bertulis
Pengguna Data memperakui penerimaan
Pengguna Data membuat pengesahan:
1. mengenal pasti / kuasa pemohon;
2. penyerahan dokumen yang diperakui untuk menyokong hak pemohon untuk meminta bagi pihak Subjek Data (jika perlu);
3. Data Peribadi yang perlu diperbetulkan telah dinyatakan dengan jelas
Menolak permohonan dan menyatakan sebab penolakan. Di mana sesuai, minta maklumat lanjut
Proses PPD dan membalas dalam masa dua puluh satu (21) hari
Memberikan Subjek Data dengan: maklumat tentang Data Peribadi yang sedang diproses; dan (jika diminta) berikan salinan Data Peribadi
Memberitahu Subjek Data secara bertulis sebab kelewatan
Memberitahu Subjek Data secara bertulis tentang keengganan untuk mematuhi PPD berdasarkan sebab dalam 2.109 dan nyatakan sebab-sebab penolakan
35 hari
Proses PPD dan balas dalam masa empat belas hari (14) tambahan
Ambil langkah-langkah yang munasabah untuk memberitahu Pihak Ketiga

2.108 Jika Pengguna Data hanya dapat memperbetulkan sebahagian daripada Data Peribadi yang diminta, Pengguna Data mesti memberikan Subjek Data Data Peribadi yang diperbetulkan sebanyak mungkin.

Bilakah Pengguna Data Boleh Menolak PPD?

2.109 Pengguna Data mempunyai hak untuk tidak mematuhi atau menolak PPD jika:

(a) Ketidakupayaan untuk mengesahkan identiti

Pengguna Data tidak dibekalkan dengan maklumat sebagaimana yang dikehendaki oleh Pengguna Data (seperti nama, nombor kad pengenalan, alamat dan maklumat lain berkenaan Subjek Data seperti yang ditentukan oleh Pengguna Data);

(b) Ketidakupayaan untuk pengesahan pembetulan

Pengguna Data tidak dibekalkan dengan maklumat yang mencukupi, sebagaimana yang dikehendaki oleh Pengguna Data, untuk menentukan bagaimana Data Peribadi itu tidak tepat, tidak lengkap, mengelirukan dan tidak terkini;-

Contoh: *Subjek Data menghantar PPD untuk pembetulan nama tetapi tidak menyediakan dokumen sokongan untuk permohonan mereka.*

(c) Data Peribadi tidak memerlukan pembetulan

Pengguna Data tidak berpuas hati bahawa Data Peribadi yang berkaitan dengan PPD adalah tidak tepat, tidak lengkap, mengelirukan dan tidak terkini; atau

(d) PPD yang tidak tepat

Pengguna Data tidak berpuas hati bahawa pembetulan yang diminta adalah tepat, lengkap, tidak mengelirukan atau terkini.

Contoh: *Di mana Subjek Data mencari perubahan pada alamat rumah tetapi Pengguna Data mempunyai sebab untuk mempercayai bahawa pemberian alamat baru adalah satu cubaan untuk mengelakkan penyerahan saman ke atas Subjek Data.*

2.110 Pengguna Data boleh memohon untuk mendapatkan bukti sokongan sebelum membetulkan Data Peribadi.

Bagaimana jika Saya Menerima Permintaan untuk Membetulkan Ekspresi Pendapat?

2.111 Di mana PPD adalah berkaitan dengan ekspresi pendapat yang dipegang oleh Pengguna Data dan sebab di atas tidak berlaku, Pengguna Data mungkin tidak bersetuju bahawa ekspresi pendapat tersebut adalah tidak tepat, tidak lengkap, mengelirukan dan tidak terkini. Walau bagaimanapun, Pengguna Data mestilah:

(a) membuat nota tentang bagaimana ekspresi pendapat boleh dipertimbangkan oleh pemohon menjadi tidak tepat, tidak lengkap, mengelirukan atau tidak terkini;

(b) lampirkan nota kepada Data Peribadi yang mencurigakan (sebagai contoh, melampirkan nota ke fail fizikal yang mengandungi Data Peribadi) atau mengekalkan nota itu secara berasingan;

(c) memastikan bahawa nota tersebut dibawa ke perhatian seseorang yang ingin menggunakan ekspresi pendapat dan memastikan agar nota tersebut boleh didapati untuk diperiksa; dan

Contoh: *Nota tersebut boleh dimasukkan sebagai sistem pop-up untuk memberitahu orang ramai yang mengakses Data Peribadi tentang pendapat yang berbeza berkenaan dengan Data Peribadi yang mencurigakan .*

(d) melampirkan salinan nota bertulis memberitahu Subjek Data tentang penolakan Pengguna Data untuk mematuhi PPD.

Bolehkah saya mengenakan Yuran?

2.112 Pengguna Data tidak berhak mengenakan yuran untuk PPD.

Penyimpan Rekod

2.113 Pengguna Data harus mengekalkan rekod untuk semua PPD yang diterima dan keputusan yang dibuat dalam mematuhi atau tidak mematuhi setiap PPD. Ini akan membolehkan Pengguna Data untuk menjawab sebarang pertanyaan daripada Subjek Data dan / atau Pengguna Data bersedia sekiranya penyiasatan dijalankan oleh Pesuruhjaya.

2.114 Sebagai amalan yang baik, Pengguna Data harus mengekalkan fail untuk setiap PPD dengan maklumat yang berikut:

(a) salinan PPD;

(b) rekod pengesahan identiti bagi seseorang yang telah diberi kuasa untuk memohon bagi pihak Subjek Data;

(c) salinan setiap surat menyurat berkaitan dengan PPD;

(d) rekod setiap keputusan yang dibuat berkenaan dengan PPD; dan

(e) salinan Data Peribadi yang telah diperbetulkan dan telah dihantar kepada Subjek Data atau seseorang yang telah diberi kuasa.

2.115 Contoh Borang PPD seperti dalam **Lampiran 6: Borang Permohonan Akses Data / Borang Permohonan Pembetulan Data.**

Tataamalan

2.116 Adalah dicadangkan bahawa Pengguna Data melaksanakan polisi dan prosedur yang berkaitan dengan kaedah untuk memastikan Subjek Data mempunyai cara untuk menghubungi Pengguna Data bagi memperbetulkan Data Peribadi mereka.

(H) Prinsip Akses (Seksyen 12 APDP)

2.117 Di bawah Prinsip Akses, Subjek Data mempunyai hak untuk memohon akses kepada Data Peribadi mereka dan hak untuk membetulkan Data Peribadi mereka yang tidak tepat, tidak lengkap, mengelirukan dan tidak terkini.

2.118 Pengguna Data dikehendaki untuk memberi maklum balas kepada sebarang Permintaan Akses Data (**"PAD"**) untuk mematuhi APDP.

2.119 Subjek Data hanya boleh mengakses Data Peribadi mereka sahaja. Subjek Data tidak boleh diberi kebenaran untuk mengakses Data Peribadi orang lain, kecuali seperti yang telah ditetapkan dibawah Kod ini.

2.120 Pengguna Data mempunyai hak untuk menolak sebarang PAD yang dihantar oleh Subjek Data. Pengguna Data boleh mengenakan caj yang sesuai untuk menyelesaikan permintaaan tersebut. Ini diterangkan dengan lebih lanjut seperti di bawah.

Pengecualian

2.121 Pengguna Data tidak dikehendaki untuk mematuhi PAD di mana Data Peribadi diproses:

(a) untuk pencegahan atau pengesanan atau untuk tujuan penyiasatan;

(b) untuk kebimbangan atau pendakwaan pesalah;

(c) untuk penilaian atau kutipan cukai atau duti atau pengenaan lain yang serupa;

(d) untuk penyediaan statistik atau menjalankan penyelidikan dengan syarat Data Peribadi tidak diproses untuk sebarang tujuan lain dan keputusan statistik dan penyelidikan tidak disebutkan;

(e) untuk tujuan atau berhubung dengan sebarang perintah atau penghakiman mahkamah; atau

(f) untuk tujuan menjalankan fungsi pengawalseliaan.

Bagaimanakah PAD berfungsi?

2.122 Subjek Data membuat PAD secara bertulis kepada Pengguna Data. PAD mungkin untuk:

(a) meminta maklumat Data Peribadi yang diproses oleh Pengguna Data; atau

(b) telah mengkomunikasikan kepada Subjek Data salinan Data Peribadi dalam bentuk yang mudah difahami. Data Subjek mesti memahami maklumat yang dibekalkan tanpa perlu merujuk semula kepada Pengguna Data untuk penjelasan.

2.123 Setelah menerima PAD, Pengguna Data mesti memperakui permintaan.

2.124 Selepas memperakui penerimaan dan mengesahkan bahawa DAR tersebut lengkap, Pengguna Data mesti menyampaikan maklumat yang diminta dan / atau salinan Data Peribadi kepada Subjek Data (jika perlu) dalam masa dua puluh satu (21) hari selepas tarikh penerimaan PAD.

2.125 Setelah tempoh dua puluh satu (21) hari telah berlalu dan Pengguna Data masih belum berjaya mematuhi dalam tempoh tersebut, Pengguna Data:

(a) mesti memberitahu Subjek Data secara bertulis tentang kelewatan dan sebab-sebab kelewatan dan lanjutan yang tidak lebih dari empat belas (14) hari akan diberikan secara automatik kepada Pengguna Data; atau

(b) mesti memberitahu Subjek Data jika ia mempunyai sebab untuk tidak mematuhi PAD.

2.126 Jika 2.125(a) digunakan pakai, Pengguna Data mesti mematuhi PAD dalam tempoh lanjutan empat belas (14) hari.

Apakah Syarat untuk PAD yang Sah?

2.127 Peraturan menyatakan bahawa di mana Subjek Data tidak memerlukan salinan Data Peribadi, Subjek Data mesti memaklumkan kepada Pengguna Data secara bertulis apabila mengemukakan PAD. Untuk memudahkan hal ini, adalah dicadangkan bahawa Pengguna Data memberikan pilihan kepada Subjek Data semasa membuat PAD sama ada Subjek Data:

(a) semata-mata ingin mengesahkan sama ada atau tidak Pengguna Data mengekalkan sebarang Data Peribadi daripada Subjek Data dan jenis Data Peribadi yang dipegang oleh Pengguna Data; atau

(b) ingin memberikan salinan Data Peribadi yang dipegang oleh Pengguna Data.

2.128 APDP tidak menyatakan format tertentu. Walau bagaimanapun, ia mesti:

(a) secara betulis;

(b) disertakan dengan bayaran yang ditetapkan dibawah Yuran Peraturan melainkan dikecualikan oleh Pengguna Data;

(c) mengandungi maklumat yang diperlukan untuk mengkehendaki Pengguna Data mencari Data Peribadi. Sebagai contoh, Subjek Data mungkin memberi maklumat tentang nama, nombor kad pengenalan atau nombor pasport, alamat dan nombor akaun;

(d) secara khusus. Permintaan untuk "semua Data Peribadi" tidak akan dipertimbangkan sebagai DAR yang betul;

(e) di mana permintaan dibuat bagi pihak Subjek Data, dokumen yang telah disahkan perlu dikemukakan untuk memberikan hak kepada Subjek Data untuk membuat permintaan.

2.129 Jika sebarang syarat-syarat ini tidak dipenuhi, Pengguna Data harus mengembalikan PAD kepada Subjek Data dan meminta untuk menghantar semula syarat-syarat yang tidak dipenuhi.

Bagaimana jika saya menerima permintaan secara lisan ?

2.130 Setelah menerima permintaan lisan, Pengguna Data harus memberi panduan kepada Subjek Data tentang cara yang betul untuk membuat PAD.

Bolehkah PAD dibuat bagi pihak Subjek Data ?

2.131 PAD boleh dibuat bagi pihak Subjek Data. Khususnya:

(a) di mana Subjek Data adalah dibawah umur lapan belas (18) tahun, ibubapa, penjaga atau orang yang dipertanggungjawabkan sebagai penjaga untuk Subjek Data boleh membuat PAD;

(b) di mana Subjek Data tidak mampu menguruskan hal ehwal sendiri, seseorang yang dilantik oleh mahkamah untuk menguruskan hal ehwal Subjek Data atau seseorang yang diberi kuasa secara bertulis oleh Subjek Data untuk membuat PAD; atau

(c) dalam kes yang lain, seseorang yang diberi kuasa secara bertulis oleh Subjek Data boleh membuat PAD bagi pihak Subjek Data.

Bagaimana jika saya menerima PAD untuk pelbagai akaun?

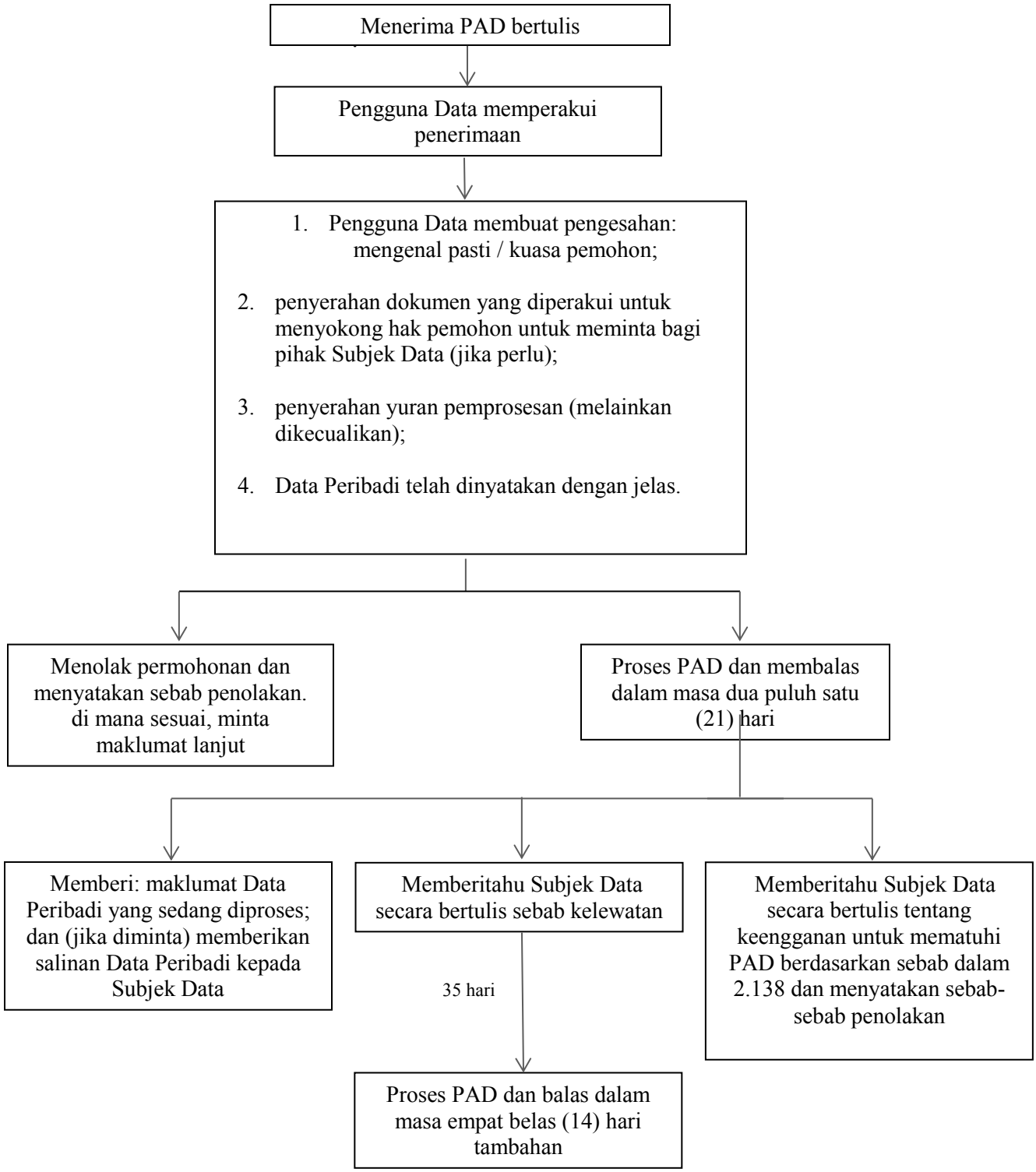
2.132 di mana Subjek Data mempunyai akaun yang berasingan dengan Pengguna Data, Pengguna Data mungkin memerlukan PAD yang berasingan untuk setiap akaun.

Bagaimana dengan Data Peribadi yang telah diarkibkan?

2.133 Subjek Data tidak mempunyai hak untuk mengakses Data Peribadi yang dikekalkan untuk tujuan sandaran dan arkib.

Apakah prosedur untuk memproses PAD?

2.134 Carta di bawah menunjukkan langkah-langkah yang perlu diambil oleh Pengguna Data setelah menerima PAD.



2.135 Jika Pengguna Data hanya boleh mencari sebahagian daripada Data Peribadi yang diminta, Pengguna Data mesti memberi Data Peribadi sebanyak mana yang boleh kepada Subjek Data.

2.136 di mana Data Peribadi terkandung dalam bentuk video atau audio, Pengguna Data boleh:

(a) mengkomunikasikan rakaman audio sebagai transkrip bertulis atau memberi Data Peribadi dalam bentuk audio (contoh: wmv atau mpeg); atau

(b) mengkomunikasikan rakaman video (termasuk imej CCTV) sebagai turutan kronologi imej atau rakaman video yang disunting di mana identiti pihak ketiga telah diselindungkan.

Apakah yang akan Berlaku jika Pengguna Data tidak mematuhi PAD?

2.137 Subjek Data mempunyai hak untuk membuat aduan kepada Pesuruhjaya jika Pengguna Data tidak mematuhi PAD. Walau bagaimanapun, Pengguna Data boleh memilih untuk tidak mematuhi PAD jika ia mempunyai sebab yang sah untuk berbuat sedemikian, seperti yang digariskan dalam APDP.

Bilakah Pengguna Data boleh menolak PAD?

2.138 Pengguna Data mempunyai hak untuk tidak mematuhi atau menolak PAD jika:

(a) Ketidakupayaan untuk mengesahkan identiti

Pengguna Data tidak diberikan maklumat sebagaimana yang dikehendaki (sebagai contoh, nama, nombor kad pengenalan, alamat dan maklumat lain yang berkenaan dengan Subjek Data seperti yang ditentukan oleh Pengguna Data) untuk mengenal pasti identiti Subjek Data atau di mana PAD yang dikemukakan oleh seseorang yang diberi kuasa, mengenal pasti hubungan orang tersebut kepada Subjek Data;

(b) Ketidakupayaan untuk mengesahkan lokasi Data Peribadi

Pengguna Data tidak dibekalkan dengan maklumat yang mencukupi oleh Subjek Data untuk menentukan lokasi sebenar Data Peribadi;

(c) Beban yang tidak seimbang

Beban atau perbelanjaan untuk memberikan akses kepada Data Peribadi tidak seimbang dengan risiko kepada privasi Subjek Data (sebagai contoh, jika masa dan kos yang akan ditanggung oleh Pengguna Data adalah lebih besar daripada kepentingan data yang diminta menerusi PAD);

(d) Penzahiran yang lain

Pengguna Data tidak dapat mematuhi PAD tanpa Menzahirkan Data Peribadi orang lain. Dalam situasi ini, Pengguna Data boleh:

(i) tidak mendedahkan nama pihak ketiga dalam Data Peribadi;

(ii) mencari persetujuan pihak ketiga jika praktikal; atau

(iii) menentukan sama ada munasabah atau tidak untuk menzahirkan Data Peribadi tanpa persetujuan pihak ketiga.

(e) Perintah Mahkamah

Memberi akses yang mana boleh melanggar perintah mahkamah;

(f) Kerahsiaan

Memberi akses yang mana boleh menzahirkan maklumat komersial yang sulit;

(g) Peraturan

Akses sedemikian adalah dikawal oleh undang-undang selain dari APDP, (sebagai contoh, Akta Suruhanjaya Penerbangan Malaysia 2015); atau

2.139 Di mana Pengguna Data mempunyai sebab untuk menolak, Pengguna Data boleh memilih untuk menolak untuk memberi semua atau sesetengah Data Peribadi, bergantung kepada keadaan.

Bolehkah saya mengenakan yuran ?

2.140 Selaras dengan Peraturan Yuran, Pengguna Data berhak untuk mengenakan yuran kepada Subjek Data untuk setiap PAD yang dihantar. Yuran maksimum yang perlu dibayar oleh Subjek Data untuk penyerahan PAD adalah:

Item	Deskripsi	Yuran maksimum (RM)
(a)	Untuk Data Peribadi dengan salinan	10
(b)	Untuk Data Peribadi tanpa salinan	2
(c)	Untuk Data Peribadi Sensitif dengan salinan	30
(d)	Untuk Data Peribadi Sensitif tanpa salinan	5

Menyimpan Rekod

2.141 Pengguna Data harus mengekalkan semua rekod PAD yang diterima dan juga keputusan untuk mematuhi atau tidak mematuhi untuk setiap PAD. Ini membolehkan Pengguna Data menjawab sebarang pertanyaan daripada Subjek Data dan / atau sediakan Pengguna Data sekiranya penyiasatan dijalankan oleh Pesuruhjaya.

2.142 Sebagai amalan yang baik, Pengguna Data harus mengekalkan fail untuk setiap PAD dengan maklumat seperti berikut:

(a) salinan PAD;

(b) rekod pengesahan identiti oleh seseorang yang diberikan kuasa untuk membuat permohonan bagi pihak Subjek Data;

(c) semua salinan surat menyurat berkenaan dengan PAD;

(d) rekod sebarang keputusan yang dibuat berkenaan dengan PAD; dan

(e) salinan Data Peribadi yang dihantar kepada Subjek Data atau orang yang diberikan kuasa.

2.143 Sampel Borang PAD boleh dirujuk dalam **Lampiran 6: Borang Permintaan Akses Data / Borang Permintaan Pembetulan Data.**

3.0 Hak-Hak Subjek Data

(A) Hak untuk Menghalang Pemprosesan Data Peribadi Yang Mungkin Menyebabkan Kerosakan atau Kesusahan (Seksyen 42 APDP)

3.1 Subjek Data boleh, melalui notis bertulis, memerlukan Pengguna Data untuk:

(a) menghentikan pemprosesan Data Peribadi; atau

(b) tidak memulakan pemprosesan Data Peribadi,

di mana pemprosesan akan menyebabkan atau mungkin menyebabkan kerosakan yang besar dan tidak wajar atau kesusahan kepada Subjek Data atau orang lain.

Apakah "substansial" atau "diwajarkan"?

3.2 "Kerosakan substansial", "kebimbangan substansial" dan "ketidakwajaran" tidak ditakrifkan di bawah APDP. Walau bagaimanapun, dalam kebanyakkan kes:

(a) "kerosakan substansial" termasuk kerugian kewangan yang dialami oleh Subjek Data;

(b) "kebimbangan substansial" termasuk trauma secara emosi atau mental yang dialami oleh Subjek Data; dan

(c) "ketidakwajaran" bermaksud kerosakan atau kesusahan yang dialami oleh Subjek Data yang tidak boleh dijustifikasikan.

Bilakah permintaan boleh ditolak ?

3.3 Subjek Data tidak mempunyai hak untuk menghalang pemprosesan di mana:

(a) Subjek Data telah memberikan persetujuan untuk pemprosesan; atau

(b) pemprosesan tersebut adalah perlu;

(i) untuk melaksanakan kontrak yang dimasuki oleh Subjek Data;

(ii) mengambil langkah-langkah di atas permintaan Subjek Data dengan tujuan untuk memasuki kontrak;

(iii) untuk mematuhi tanggungjawab undang-undang yang dikenakan kepada Pengguna Data, selain daripada kontrak; atau

(iv) untuk melindungi kepentingan Subjek Data, seperti perkara yang melibatkan kehidupan, kematian atau keselamatan Subjek Data.

Apakah tempoh masa yang harus dipatuhi oleh Pengguna Data?

3.4 Setelah menerima notis bertulis untuk menghentikan pemprosesan atau tidak memulakan pemprosesan Data Peribadi, Pengguna Data mesti memberi notis bertulis kepada Subjek Data dalam tempoh masa dua puluh satu (21) hari penerimaan notis tersebut yang menyatakan:

(a) bahawa Pengguna Data telah mematuhi atau berhasrat untuk mematuhi notis tersebut;

(b) jika Pengguna Data tidak berhasrat untuk mematuhi permintaan tersebut, alasan perlu diberikan untuk keputusan tersebut;

(c) di mana berkenaan, nyatakan sebab-sebab permintaan tersebut adalah tidak wajar, dan sejauh mana beliau telah mematuhi atau berhasrat untuk mematuhi permintaan tersebut.

Bagaimanakah Pengguna Data menilai permintaan tersebut?

3.5 Pengguna Data boleh mempertimbangkan perkara seperti berikut apabila membuat keputusan sama ada untuk mematuhi permintaan tersebut:

(a) Adakah permintaan Subjek Data untuk tujuan yang sah? Subjek Data harus memberikan sebab-sebab yang sah kerana kerosakan atau kesusahan yang terjadi adalah "substansial".

(b) Adakah kerosakan dan kesusahan tidak wajar? Ini berhubung kait sama ada Subjek Data telah memberikan sebab-sebab yang sah untuk permintaan tersebut.

Hak Subjek Data

3.6 Di mana Pengguna Data tidak mematuhi notis tersebut, Subjek Data boleh memohon kepada Pesuruhjaya untuk meminta Pengguna Data mematuhi notis tersebut.

3.7 Jika Pesuruhjaya berpuas hati bahawa permintaan Subjek Data adalah wajar, Pesuruhjaya boleh mengarahkan Pengguna Data untuk mamatuhi permintaan tersebut.

(B) Hak untuk Menghalang Pemprosesan Data Peribadi untuk Tujuan Pemasaran Langsung (Seksyen 43 APDP)

3.8 Subjek Data mempunyai hak untuk, melalui notis bertulis, memerlukan Pengguna Data untuk menghentikan atau tidak memulakan pemprosesan Data Peribadi untuk tujuan pemasaran langsung. Bahagian B, Bab 5 menghuraikan dengan lebih lanjut tentang praktis sektor penerbangan berkenaan dengan pemasaran langsung.

3.9 Pengguna Data mesti mematuhi permintaan tersebut dalam tempoh masa yang munasabah.

3.10 Permohonan Subjek Data secara bertulis mesti dikomunikasikan ke seluruh organisasi untuk memastikan bahawa permintaan Subjek Data dipatuhi. Di mana ada keperluan untuk Pengguna Data mengemas kini sistem dan pengkalan yang berkenaan untuk mencerminkan arahan Subjek Data. Pengguna Data secara kebiasaannya diharapkan dapat mematuhi permintaan Subjek Data dalam tempoh tiga (3) bulan.

3.11 Di mana Subjek Data membuat permintaan secara bertulis memohon untuk menerima beberapa bahan pemasaran langsung dan bukan yang lain, Pengguna Data boleh memilih untuk tidak memberikan Subjek Data dengan semua bahan pemasaran langsung, sekiranya sistem mereka tidak berupaya untuk membezakan antara jenis bahan pemasaran yang berlainan.

Berurusan dengan Pemasaran Langsung ("Direct Marketing")

3.12 Pemasaran langsung ditakrifkan sebagai "komunikasi dalam sebarang bentuk bahan pengiklanan atau pemasaran yang ditujukan kepada pelanggan tertentu".

3.13 Pengguna Data mengumpul banyak maklumat peribadi. Pemprosesan maklumat yang banyak oleh Pengguna Data membawa kepada potensi jualan silang dan sasaran tingkah laku untuk mengambil kesempatan terhadap bidang yang belum diterokai sebelum ini untuk menjana pendapatan.

3.14 Pemasaran langsung mesti mengandungi bahan pengiklanan atau pemasaran **yang ditujukan kepada pelanggan tertentu.** Bahan pemasaran yang tidak ditujukan kepada seseorang individu yang tertentu tetapi dihantar kepada semua pelanggan oleh Pengguna Data tidak akan dianggap sebagai pemasaran langsung.

Contoh*: Mempamerkan sepanduk tawaran promosi kepada pelanggan syarikat penerbangan di mana ia boleh dilihat oleh pelanggan berpotensi yang menggunakan laman web syarikat penerbangan tersebut.*

Apakah keperluan untuk pemasaran langsung di bawah APDP?

3.15 Pesuruhjaya tidak mengeluarkan garis panduan rasmi tentang urusan pemasaran langsung. Walau bagaimanapun, adalah dicadangkan bahawa Pengguna Data mematuhi amalan-amalan seperti berikut:-

Persetujuan

(a) Pengguna Data mesti memperolehi persetujuan Subjek Data untuk menggunakan Data Peribadi mereka untuk pemasaran langsung melalui surat pos. Untuk pemasaran langsung melalui elektronik, Subjek Data mesti memberikan **persetujuan yang jelas**. **Lampiran 3: Prinsip Am** menyediakan templat persetujuan untuk pemasaran langsung.

Pilihan keluar

(b) APDP memberikan hak kepada Subjek Data untuk menarik balik persetujuan untuk memproses pemasaran langsung. Pengguna Data harus memastikan bahawa Subjek Data boleh menarik balik persetujuan pada bila-bila masa:

(i) Subjek Data harus mempunyai pilihan untuk keluar daripada pemasaran langsung pada peringkat awal pengumpulan, sebagai contoh melalui kotak untuk menanda pilihan keluar;

(ii) hak untuk pilihan keluar mesti disediakan dalam setiap mesej pemasaran yang berikut. Sebagai contoh, Subjek Data mungkin akan diberi pautan di mana mereka boleh klik untuk "berhenti melanggan" untuk komunikasi pemasaran yang selanjutnya; dan

(iii) Notis Privasi Pengguna Data harus menyatakan dengan jelas kaedah lain di mana Subjek Data boleh menghubungi Pengguna Data untuk menarik balik persetujuan mereka untuk pemasaran langsung.

Adalah dicadangkan bahawa Pengguna Data membangunkan sistem untuk menguruskan permintaan penolakan tersebut bagi memastikan semua permintaan penolakan dicatat dengan tepat dan bahan pemasaran tidak dihantar kepada Subjek Data. Pengguna Data juga boleh membangunkan prosedur operasi standard dan polisi yang berkaitan dengan pengurusan permintaan tersebut.

Sumber Data Peribadi

(c) Data Peribadi mesti diperolehi semasa urusan perniagaan yang terdahulu dengan Subjek Data, seperti penjualan produk atau perkidmatan.

Dimaklumkan

(d) Subjek Data mesti dimaklumkan tentang identiti Pengguna Data, bahawa Data Peribadi Subjek Data akan digunakan untuk pemasaran langsung, dan sama ada Data Peribadi akan dizahirkan kepada pihak ketiga lain yang berkenaan dengan pemasaran langsung.

Produk / Perkhidmatan yang Serupa

(e) pemasaran langsung mesti dihadkan kepada produk dan perkidmatan yang serupa.

Bolehkah saya mendapatkan Data Peribadi daripada sumber yang tersedia secara umum?

3.16 Pengguna Data tidak boleh menggunakan Data Peribadi yang diperolehi daripada sumber yang tersedia secara umum seperti maklumat yang dijumpai di Facebook atau internet untuk tujuan pemasaran langsung kerana Subjek Data tidak menyediakan maklumat tersebut secara terbuka untuk tujuan menerima sebarang komunikasi permasaran langsung yang tidak diingini dan tidak memberikan persetujuan mereka untuk menerima komunikasi sedemkikian.

Bolehkah saya melantik pihak ketiga untuk menjalankan pemasaran langsung bagi pihak saya?

3.17 Pengguna Data boleh melantik Pemproses Data pihak ketiga untuk menjalankan pemasaran langsung bagi pihaknya. Walau bagaimanapun, ia harus memastikan bahawa terdapat perjanjian di antara Pengguna Data dan Pemproses Data. Syarikat penerbangan boleh menggunakan contoh klausa yang disediakan dalam **Lampiran 5: Data Peribadi yang Dizahirkan atau Diterima daripada Pihak Ketiga.**

(C) Hak Untuk Menarik Balik Persetujuan untuk Pemprosesan Data Peribadi (Seksyen 38 APDP)

3.18 Subjek Data boleh menarik balik persetujuan mereka untuk memproses Data Peribadi pada bila-bila masa dengan memberikan notis bertulis kepada Pengguna Data.

3.19 Pengguna Data mesti menghentikan pemprosesan Data Peribadi Subjek Data sejurus penerimaan dan pengesahan notis. Walau bagaimanapun, Pengguna Data tidak perlu berhenti memproses data sehingga penolakan persetujuan akan menjejaskan hak dan tanggungjawab Pengguna Data di bawah kontrak atau undang-undang.

***Contoh**: Hak dan tanggungjawab tersebut termasuk:*

(a) hak untuk dibayar kepada perkhidmatan yang telah diberikan, sebagai contoh, penyelesaian tempahan atau invois cukai, atau bayaran tertunggak;

(b) hak untuk membawa dan mengekalkan prosiding undang-undang terhadap Subjek Data (sebagai contoh: di mana penumpang telah membuat aduan atau memulakan prosiding undang-undang terhadap syarikat penerbangan, syarikat penerbangan boleh menyimpan Data Peribadi untuk memastikan ia mempunyai rekod transaksi yang lengkap, di mana rekod termasuk Data Peribadi (contoh nama, nombor pasport / nombor kad pengenalan, alamat, dll);

(c) hak untuk memulakan atau meneruskan penyiasatan dalaman yang melibatkan Subjek Data;

(d) tanggungjawab untuk mengekalkan Data Peribadi untuk jangka masa sebagaimana yang dikehendaki di bawah undang-undang yang berkaitan; sebagai contoh, untuk mengekalkan Data Peribadi di bawah Akta Arkib Kebangsaan 2003; dan

(e) pengendalian audit dalaman, pengurusan risiko dan / atau memenuhi keperluam undang-undang atau keperluan melaporkan pengawaseliaan.

4.0 Isu-isu Khusus

A) Menguruskan Pemindahan Data Peribadi ke Luar Negara

4.1 Pengguna Data kebiasaannya beroperasi dalam beberapa bidang kuasa dan mungkin memerlukan pemindahan Data Peribadi kepada bidang kuasa di luar Malaysia, antara lain, rakan kongsi syarikat penerbangan, anak syarikat di luar negara atau pelayar sandaran. Di dalam APDP terkandung sekatan tentang pemindahan Data Peribadi di luar negara kecuali Subjek Data telah bersetuju untuk pemindahan tersebut.

4.2 Di mana Subjek Data tidak bersetuju untuk pemindahan, APDP membenarkan pemindahan ke luar Negara di mana:

(a) pemindahan tersebut adalah perlu untuk perlaksanaan kontrak di antara Pengguna Data dan Subjek Data;

(b) pemindahan tersebut adalah perlu untuk melaksanakan atau menyelesaikan kontrak di antara Pengguna Data dan pihak ketiga di mana ia telah dimasuki di atas permintaan atau untuk kepentingan Subjek Data;

***Contoh**: Di mana Pengguna Data perlu memindahkan Data Peribadi kepada rakan kongsi syarikat penerbangan untuk memastikan penerbangan sambungan tersedia untuk keperluan perjalanan penumpang.*

(c) pemindahan tersebut adalah untuk prosiding undang-undang atau mendapatkan nasihat perundangan atau menubuhkan, melaksanakan atau mempertahankan hak perundangan;

(d) Pengguna Data mempunyai alasan yang munsabah untuk mempercayai bahawa di dalam semua keadaan kes:

(i) pemindahan tersebut adalah untuk mengelakkan atau pengurangan tindakan tidak baik terhadap Subjek Data;

(ii) adalah tidak praktikal untuk mendapatkan persetujuan daripada Subjek Data secara bertulis untuk pemindahan tersebut; dan

(iii) sekiranya praktikal untuk memperolehi persetujuan tersebut, Subjek Data akan memberikan persetujuannya.

(e) Pengguna Data telah mengambil semua langkah berjaga-jaga yang munasabah dan menjalankan penilaian cermat untuk memastikan bahawa Data Peribadi tidak akan diproses dibidang kuasa yang lain dengan melanggar standard yang ditetapkan di dalam APDP;

***Contoh**: Pengguna Data telah menjalankan penilaian cermat ke atas pembekal perkhidmatan pihak ketiga yang terpilih dan telah memasuki perjanjian pemindahan data dengan pembekal perkhidmatan pihak ketiga.*

(f) pemindahan tersebut adalah perlu untuk melindungi kepentingan Subjek Data; atau

(g) pemindahan tersebut adalah perlu kerana ia melibatkan kepentingan awam seperti yang ditentukan oleh Menteri.

Tataamalan

4.3 Untuk membolehkan pemindahan Data Peribadi ke luar negara, cara pengecualian yang paling praktikal yang Pengguna Data boleh bergantung adalah dengan memperolehi persetujuan Subjek Data untuk pemindahan tersebut. Persetujuan boleh diperolehi melalui Notis Privasi dan bahasa persetujuan. Pengguna Data boleh melakukannya dengan menangani isu pemindahan melalui Notis Privasi dan memaklumkan kepada Subjek Data bahawa Data Peribadi mereka mungkin dipindahkan ke luar Negara.

4.4 Adalah dicadangkan bahawa Pengguna Data menjalankan penilaian cermat ke atas penerima Data Peribadi dan memastikan jaminan yang bersesuaian diperolehi daripada penerima Data Peribadi seperti:

(a) bahawa penerima memberikan semua maklumat dan kerjasama tentang pemprosesan Data Peribadi kerana Pengguna Data mungkin memerlukannya utuk mematuhi APDP;

(b) untuk menjalankan pemprosesan hanya seperti yang diperlukan untuk memenuhi tanggungjawab kontrak kepada Pengguna Data;

(c) tidak menzahirkan Data Peribadi kepada orang lain kecuali setakat mana yang perlu untuk memenuhi tanggungjawab kontrak kepada Pengguna Data;

(d) untuk melindungi keselamatan Data Peribadi dan melaksanakan dan mengekalkan langkah keselamatan teknologi dan organisasi dan memberikan butiran yang sama kepada Pengguna Data jika diminta;

(e) tidak menyimpan Data Peribadi Subjek Data untuk tempoh yang lebih lama daripada diperlukan untuk memenuhi tanggungjawab kontrak penerima kepada Pengguna Data; dan

(f) untuk membenarkan Pengguna Data dan / atau wakilnya untuk menjalankan pemeriksaan kemudahan pemprosesan penerima Data Peribadi untuk memastikan pematuhan dengan APDP.

(B) Isu-isu Lain

Bolehkah saya mengambil gambar di majlis korporat?

4.5 Foto mengandungi imej Subjek Data yang mungkin boleh dikenal pasti identiti Subjek Data. Imej tersebut adalah berkemungkinan besar Data Peribadi.

4.6 Pengguna Data boleh mengambil gambar di majlis korporat. Walau bagaimanapun, Pengguna Data harus mengamalkan amalan seperti berikut:

(a) di mana acara tersebut adalah melalui undangan, Pengguna Data harus menyatakan dalam kad jemputan bahawa gambar akan diambil dan imej tersebut mungkin akan digunakan untuk penerbitan;

(b) jika majlis tersebut terbuka kepada orang awam, notis yang jelas harus diletakkan di pintu masuk atau resepsi tempat majlis dijalankan untuk memaklumkan kepada tetamu bahawa gambar akan diambil dan imej tersebut mungkin akan digunakan untuk penerbitan oleh Pengguna Data.

Apakah yang perlu saya lakukan jika saya menghubungi Subjek Data tetapi orang lain yang menjawab?

4.7 Pengguna Data mungkin dikehendaki menghubungi Subjek Data dalam beberapa keadaan. Jika panggilan tersebut dijawab oleh orang lain selain daripada Subjek Data, adalah dibenarkan untuk Pengguna Data memberitahu penerima panggilan tersebut identiti Pengguna Data, meminta maklumat tentang waktu kelapangan Subjek Data dan menyatakan bahawa Pengguna Data akan menghubunginya kemudian.

4.8 Pengguna Data tidak boleh menzahirkan maklumat lanjut, seperti sebarang maklumat yang berkaitan dengan nombor akaun ahli, atau sebarang jadual penerbangan.

Bagaimana dengan pemasangan CCTV?

4.9 Pengguna Data mesti mempamerkan notis yang boleh dilihat oleh pelawat premis yang memaklumkan kepada orang awam tentang operasi CCTV dan tujuan pemasangan CCTV tersebut.

4.10 Notis hendaklah:

(a) di dalam Bahasa Inggeris dan Bahasa Melayu;

(b) jelas kelihatan di semua pintu masuk dan keluar premis Pengguna Data, terutama disekitar zon pengawasan CCTV; dan

(c) menerangkan tujuan rakaman dan maklumat perhubungan orang yang bertanggungjawab untuk rakaman CCTV.

4.11 Pengguna Data boleh menggunakan contoh notis seperti:

(a) Dalam Bahasa Inggeris

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

(b) Dalam Bahasa Melayu

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

Mempamerkan Sijil Pendaftaran

4.12 Syarikat Penerbangan adalah dikehendaki untuk mendapatkan dan mempamerkan Sijil Pendaftaran asal yang dikeluarkan oleh Pesuruhjaya di ibu pejabat syarikat.

4.13 Di setiap cawangan, Pengguna Data dikehendaki untuk mempamerkan salinan Sijil Pendaftaran yang telah disahkan oleh Persuruhjaya.

4.14 Cawangan bermaksud mana-mana pejabat yang dikendalikan oleh Pengguna Data di mana interaksi berlaku dengan Subjek Data. Walau bagaimanapun, kiosk, tempat pertukaran barang dan pejabat yang tiada interaksi dengan Pengguna Data tidak dianggap sebagai "cawangan".

4.15 Pengguna Data boleh mempamerkan Sijil Pendaftaran di papan notis di dalam premis, paparan elektronik dan di laman *web* korporat Pengguna Data.

5.0 Pematuhan dalam Tataamalan

Mengekalkan Sistem APDP

5.1 Peraturan-peraturan memerlukan Pengguna untuk mengekalkan sistem Data Peribadi di mana ia mesti tersedia untuk diperiksa oleh Pesuruhjaya atau pegawai yang berkaitan. Pengguna Data mesti mengekalkan:

(a) rekod persetujuan daripada Subjek Data berkenaan dengan pemprosesan Data Peribadi oleh Pengguna Data;

(b) rekod notis bertulis yang dikeluarkan oleh Pengguna Data kepada Subjek Data;

(c) senarai penzahiran kepada Pihak Ketiga yang berkenaan dengan Data Peribadi yang telah atau sedang diproses oleh Pihak Ketiga;

(d) rekod pematuhan mengikut dengan Standard Penyimpanan;

(e) rekod pematuhan mengikut Standard Integriti Data; atau

(f) lain-lain maklumat yang berkaitan.

Polisi dan Prosedur

5.2 Melaksanakan pematuhan yang melibatkan pembuatan polisi dan prosedur yang menetapkan perkara yang boleh dilakukan dan dilarang berkenaan dengan Data Peribadi.

5.3 Selanjutnya:

(a) polisi dan prosedur ini mesti dikomunikasikan kepada kakitangan;

(b) kakitangan yang berkaitan harus dilatih tentang polisi, prosedur dan diberi pengetahuan tentang APDP, Standard dan Peraturan. Kakitangan harus dilatih tentang APDP dan polisi perlindungan data yang berkaitan apabila mereka mula menyertai syarikat;

(c) Kesedaran tentang polisi perlindungan data yang berkaitan harus menjadi sebahagian daripada setiap kakitangan Pengguna Data;

(d) Pengguna Data harus melaksanakan tahap kebenaran dan memberi akses Data Peribadi kepada kakitangan yang terpilih sahaja;

(e) klausa kerahsiaan dan kemungkinan sekatan untuk pencerobohan harus dimasukkan ke dalam perjanjian pekerjaan atau manual / buku panduan kakitangan; dan

(f) Pengguna Data harus menyediakan protokol untuk langkah-langkah yang perlu diambil menurut pencerobohan keselamatan dan pelanggaran APDP oleh kakitangan.

5.4 Pengguna Data adalah digalakkan untuk memastikan yang latihan dan / atau kesedaran yang bersesuaian disediakan untuk setiap kakitangan bagi memastikan kakitangan memahami kepentingan untuk mematuhi polisi dan prosedur tersebut. Kakitangan yang berkaitan akan dikenal pasti untuk menerima latihan khusus, seperti latihan keselamatan dan kesedaran penipuan dan mengendalikan akses data / permohonan pembetulan.

5.5 Pengguna Data harus memastikan bahawa ia mengikuti perkembangan terkini berkenaan APDP dan sentiasa memberikan latihan kepada kakitangan apabila diperlukan untuk terus mengikuti sebarang perubahan.

6.0 Pentadbiran Kod

Pematuhan dan Pemantauan

6.1 Pengguna Data mesti membuat dan melaksanakan polisi pematuhan, prosedur dan rangka kerja yang bersesuaian untuk memastikan pematuhan dengan APDP dan Kod ini.

6.2 Untuk memantau pematuhan, Pengguna Data adalah digalakkan untuk:

(a) melaksanakan pemantauan rangka kerja dalaman; dan

(b) menjalankan audit.

6.3 Jika Pengguna Data mengenal pasti kekurangan dan kelemahan dalam melaksanakan rangka kerja pematuhan, Pengguna Data harus memastikan bahawa kekurangan atau kelemahan ini telah ditangani secepat yang mungkin.

6.4 Adalah dicadangkan bahawa Pengguna Data:

(a) melaksanakan sistem pelaporan oleh orang-orang yang utama di dalam organisasi (sebagai contoh, pegawai yang bertanggungjawab untuk pematuhan APDP, ketua unit perniagaan dan kakitangan utama yang berkaitan) kepada pengurusan kanan Pengguna Data, untuk menyemak dan menilai status pelaksanaan APDP dan Kod ini. Ini akan membolehkan Pengguna Data untuk memantau isu-isu, menangani kekurangan dan memantau perkembangan Pengguna Data dalam mematuhi APDP dan Kod ini.

(b) menjalankan audit secara berkala untuk mengenal pasti isu-isu yang berkaitan dengan pematuhan APDP dan Kod ini.

6.5 Di mana perlu, Pengguna Data harus berjumpa di antara satu sama lain bagi membincangkan isu-isu yang berbangkit di bawah Kod ini dan perkara-perkara lain yang berkaitan.

Pindaan

6.6 Kod ini boleh dipinda, disemak semula atau dikemas kini untuk memasukkan semua perubahan kepada APDP. Pesuruhjaya akan memberitahu Pengguna Data secara bertulis tentang semua pindaan, semakan atau kemas kini kepada APDP.

6.7 Pindaan ke atas Kod ini boleh dibuat di mana:

(a) terdapat pindaan kepada APDP, Peraturan dan / atau Standard;

(b) Pesuruhjaya membuat pindaan di atas kehendaknya sendiri; dan / atau

(c) Pengguna Data membuat cadangan untuk pindaan kepada Pesuruhjaya berdasarkan keputusan semakan Kod ini.

6.8 Pesuruhjaya akan memasukkan butir-butir pindaan di dalam Daftar Kod Tataamalan dan akan menyediakan perkara yang sama untuk orang awam.

6.9 Setiap pindaan kepada Kod ini akan berkuatkuasa semasa pendaftarannya di dalam Daftar Kod Tataamalan .

7.0 Lampiran

LAMPIRAN 1 – DEFINISI/GLOSARI

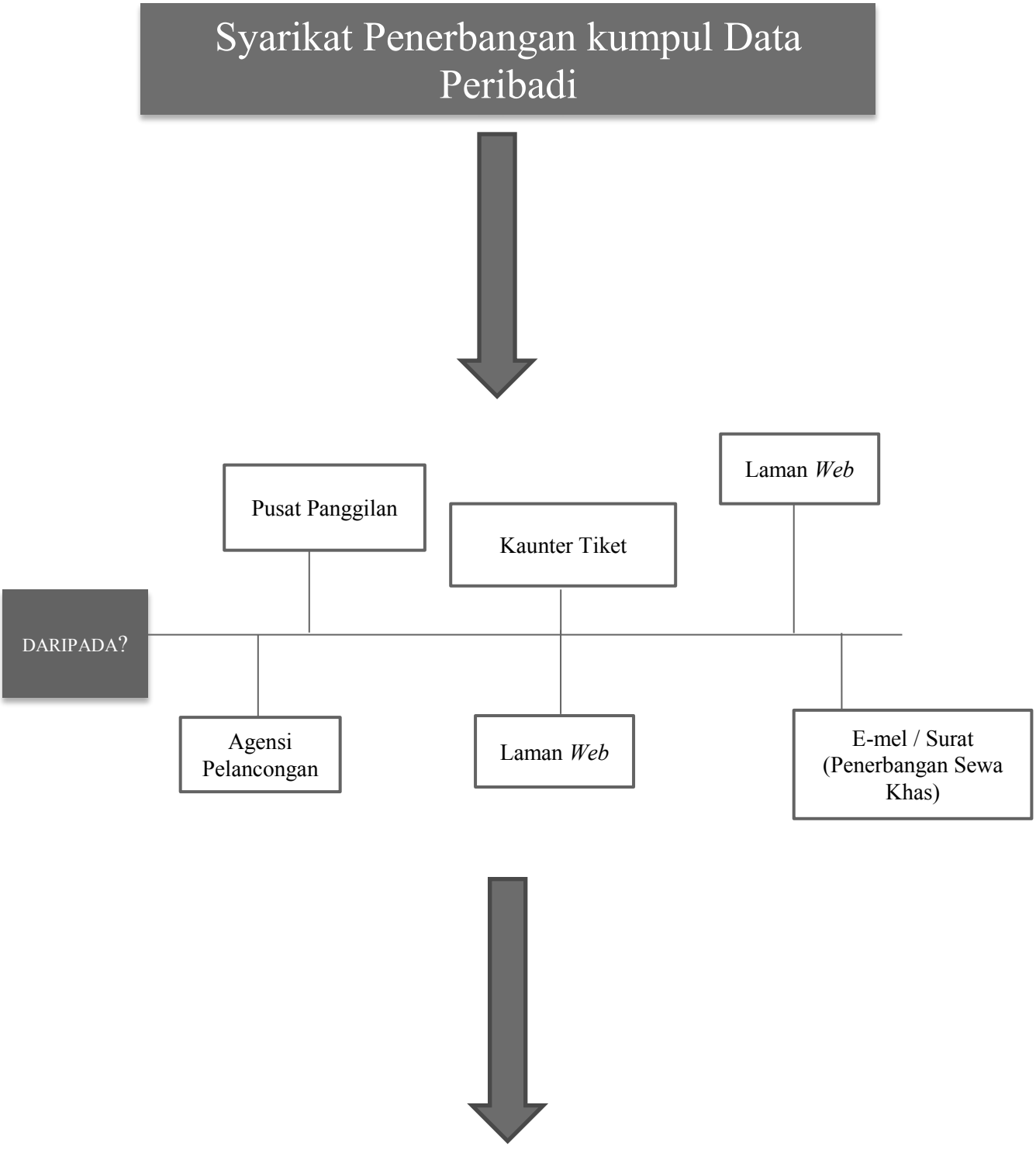
Perkataan	**Definisi**
Kod	Kod Tataamalan Perlindungan Data Peribadi ini adalah untuk Sektor Penerbangan.
Kumpul	Berkenaan dengan Data Peribadi, suatu perbuatan di mana Data Peribadi dimasukkan atau di bawah kawalan Pengguna Data.
Transaksi Komersial	Sebarang transaksi bersifat komersial, sama ada secara berkontrak atau tidak, yang merangkumi sebarang perkara yang berkaitan dengan pembekalan atau pertukaran barangan atau perkhidmatan, agensi, pelaburan, pembiayaan, perbankan dan insurans, tetapi tidak termasuk perniagaan pelaporan kredit, perniagaan yang dijalankan oleh agensi pelaporan kredit di bawah Akta Agensi Pelaporan Kredit 2010.
Pesuruhjaya	Pesuruhjaya Perlindungan Data Peribadi dilantik mengikut APDP.
Permohonan Akses Data	Permohonan bertulis yang dibuat oleh Subjek Data kepada Pengguna Data untuk mengakses Data Peribadi Subjek Data tersebut.
Permohonan Pembetulan Data	Permohonan bertulis yang dibuat oleh Subjek Data kepada Pengguna Data untuk membetulkan Data Peribadi Subjek Data tersebut.
Pemproses Data	Mana-mana orang, selain daripada kakitangan Pengguna Data, yang memproses Data Peribadi hanya bagi pihak Pengguna Data, dan tidak memproses Data Peribadi untuk tujuannya sendiri.
Subjek Data	Seseorang yang menjadi subjek Data Peribadi. Di bawah Kod ini, ia termasuk yang berikut: (a) orang yang sedang atau pernah menjadi pelanggan kepada Pengguna Data; (b) orang yang mewakili pelanggan Pengguna Data (seperti ibubapa kepada anak kecil, pemegang amanah dan wakil yang diberi kuasa); dan (c) orang yang telah dikenal pasti sebagai pelanggan berpotensi oleh Pengguna Data.
Pengguna Data	Seseorang yang sama ada bersendirian atau bersama-sama atau serupa dengan orang lain yang memproses sebarang Data Peribadi atau yang mempunyai

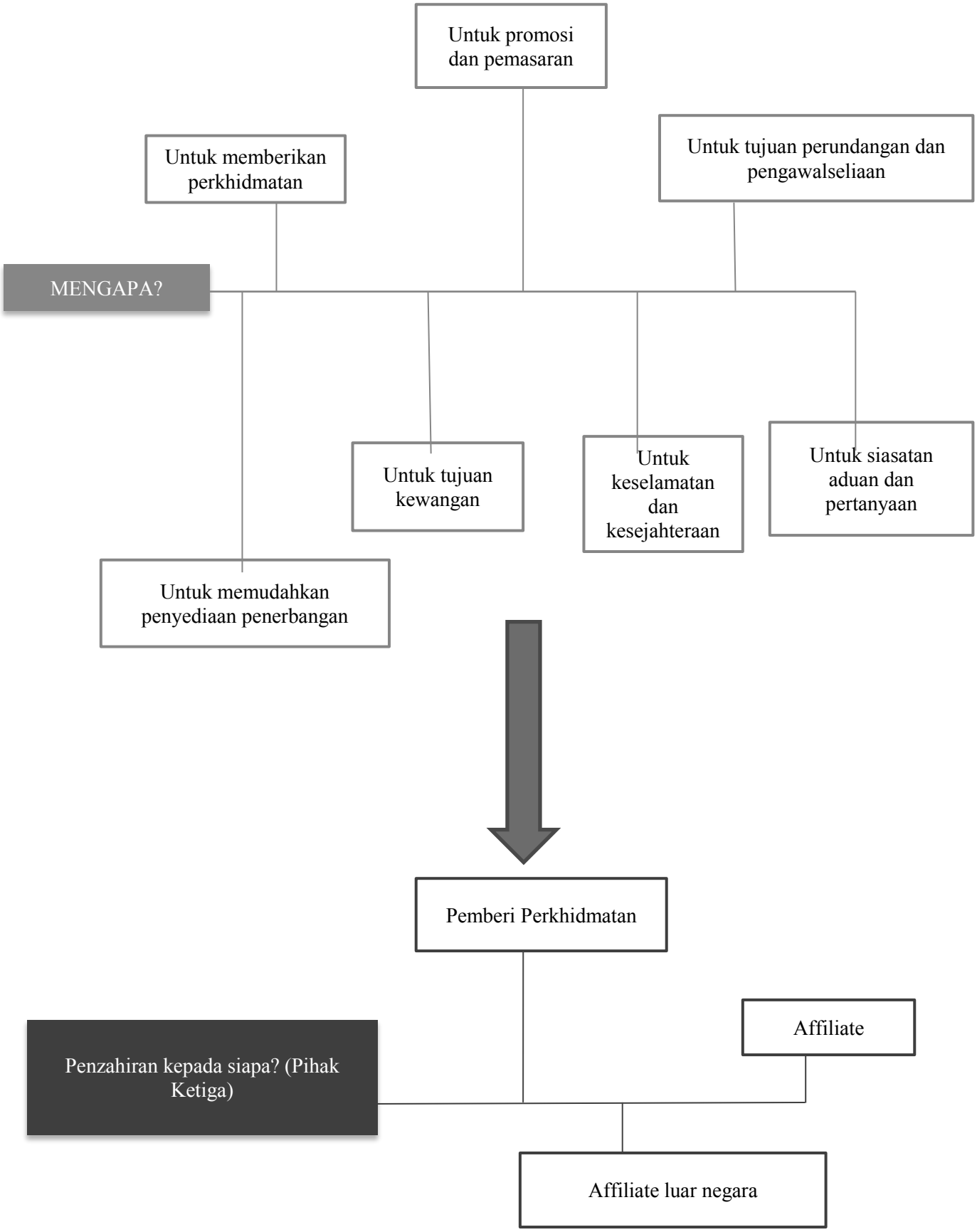
	kawalan atau membenarkan pemprosesan, tetapi tidak termasuk Pemproses Data. Di bawah Kod ini:- (a) Malaysia Airlines Berhad; (b) AirAsia Berhad; (c) AirAsia X Berhad; (d) MASWINGS Sdn. Bhd; (e) Malindo Airways Sdn Bhd; (f) Berjaya Air Sdn Bhd; dan (g) FlyFirefly Sdn Bhd.
Pemasaran Langsung	Komunikasi dengan apa cara bentuk pengiklanan atau bahan pemasaran yang ditujukan kepada orang tertentu.
Penzahiran	Berhubung dengan Data Peribadi, suatu perbuatan di mana Data Peribadi disediakan oleh Pengguna Data.
Ekspresi Pendapat	Penegasan fakta yang tidak boleh disahkan atau di dalam semua keadaan adalah tidak praktikal untuk disahkan.
Peraturan Yuran	Peraturan (Yuran) Pelindungan Data Peribadi 2013.
Memilih masuk	Merujuk kepada pilihan positif yang dilakukan oleh Subjek Data bagi memilih untuk menerima atau melanggan perkhidmatan dan / atau komunikasi pemasaran daripada Pengguna Data.
Memilih keluar	Merujuk kepada tindakan positif yang dilakukan oleh Subjek Data untuk tidak melanggan atau tidak menerima perkhidmatan dan / atau komunikasi pemasaran di mana Subjek Data telah menerimanya kerana perhubungan yang sedia ada dengan Pengguna Data.
APDP	Akta Perlindungan Data Peribadi 2010
Data Peribadi	Sebarang maklumat berkaitan dengan Transaksi Komersial, di mana: (a) diproses secara keseluruhan atau sebahagiannya dengan peralatan yang beroperasi secara automatik sebagai tindak balas kepada arahan yang diberikan untuk tujuan tersebut; (b) direkodkan untuk tujuan bahawa ia perlu diproses secara keseluruhan atau sebahagiannya dengan menggunakan peralatan tersebut; atau (c) direkodkan sebagai sebahagian daripada Sistem Pemfailan yang Berkaitan atau untuk tujuan bahawa ia perlu menjadi sebahagian daripada Sistem Pemfailan yang Berkaitan;

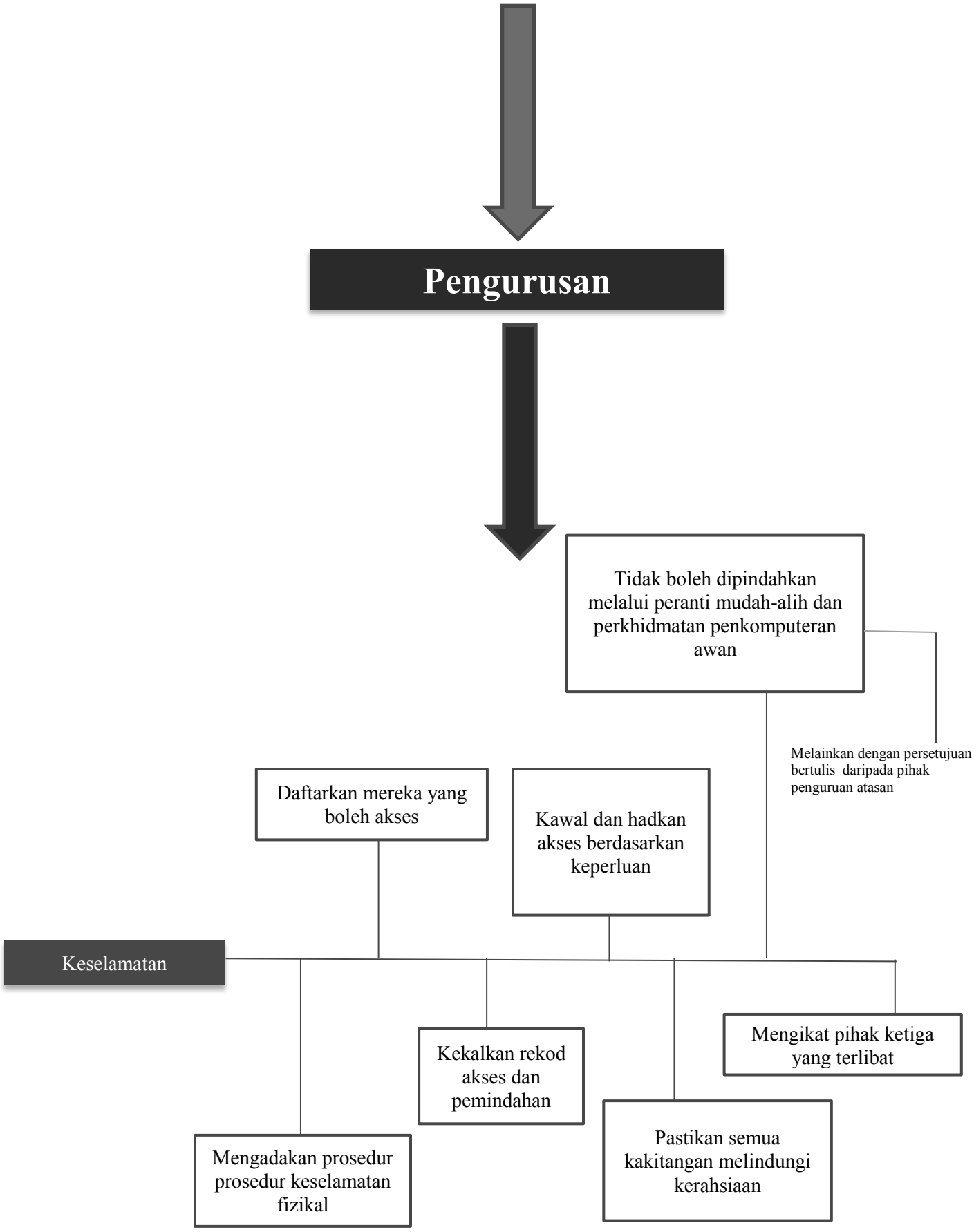
	yang berkaitan secara langsung atau tidak langsung kepada Subjek Data, yang telah dikenal pasti atau boleh dikenal pasti daripada maklumat tersebut atau daripada maklumat lain yang dimiliki oleh Pengguna Data, termasuk sebarang Data Peribadi Sensitif dan ekspresi pendapat tentang Subjek Data, tetapi tidak termasuk sebarang maklumat yang diproses untuk tujuan pelaporan kredit perniagaan yang dijalankan oleh agensi pelaporan kredit dibawah Akta Agensi Pelaporan Kredit 2010.
Notis Privasi	Notis Perlindungan Data Peribadi yang dikeluarkan oleh Pengguna Data, dan mungkin akan dipinda dari semasa ke semasa.
Proses, Semua Proses, Telah Diproses, Pemprosesan	Berhubung dengan Data Peribadi, yang bermaksud mengumpul, merekod, memegang atau menyimpan Data Peribadi atau menjalankan sebarang operasi atau menetapkan operasi keatas Data Peribadi, termasuk: (a) mengendalikan, mengadaptasi atau mengubah Data Peribadi; (b) pengambilan semula, perundingan atau penggunaan Data Peribadi; (c) penzahiran Data Peribadi melalui penghantaran, pemindahan, penyebaran atau sebaliknya menyediakan; atau (d) penyelarasan, penggabungan, pembetulan, pemadaman atau pemusnahan Data Peribadi.
Peraturan	Peraturan Perlindungan Data Peribadi 2013.
Sistem Pemfailan yang Berkaitan	Sebarang maklumat yang berkaitan dengan individu, walaupun maklumat tersebut tidak diproses dengan peralatan yang beroperasi secara automatik sebagai tindak balas kepada arahan yang diberikan bagi tujuan tersebut, maklumat tersebut adalah tersusun, sama ada secara rujukan kepada individu atau rujukan kepada kriteria yang berkaitan dengan individu, di mana maklumat khusus yang berkaitan dengan seseorang individu boleh diakses pada bila-bila masa.
Data Peribadi Sensitif	Sebarang Data Peribadi yang mengandungi maklumat tentang kesihatan atau keadaan fizikal atau mental seseorang Subjek Data, pendapat politik, kepercayaan agama atau kepercayaan lain yang serupa, perlakuan atau tuduhan perlakuan mereka tentang sebarang kesalahan atau sebarang Data Peribadi lain seperti yang ditentukan oleh Menteri melalui perintah yang disiarkan di dalam Warta.
Standard	Standard Perlindungan Data Peribadi 2015.

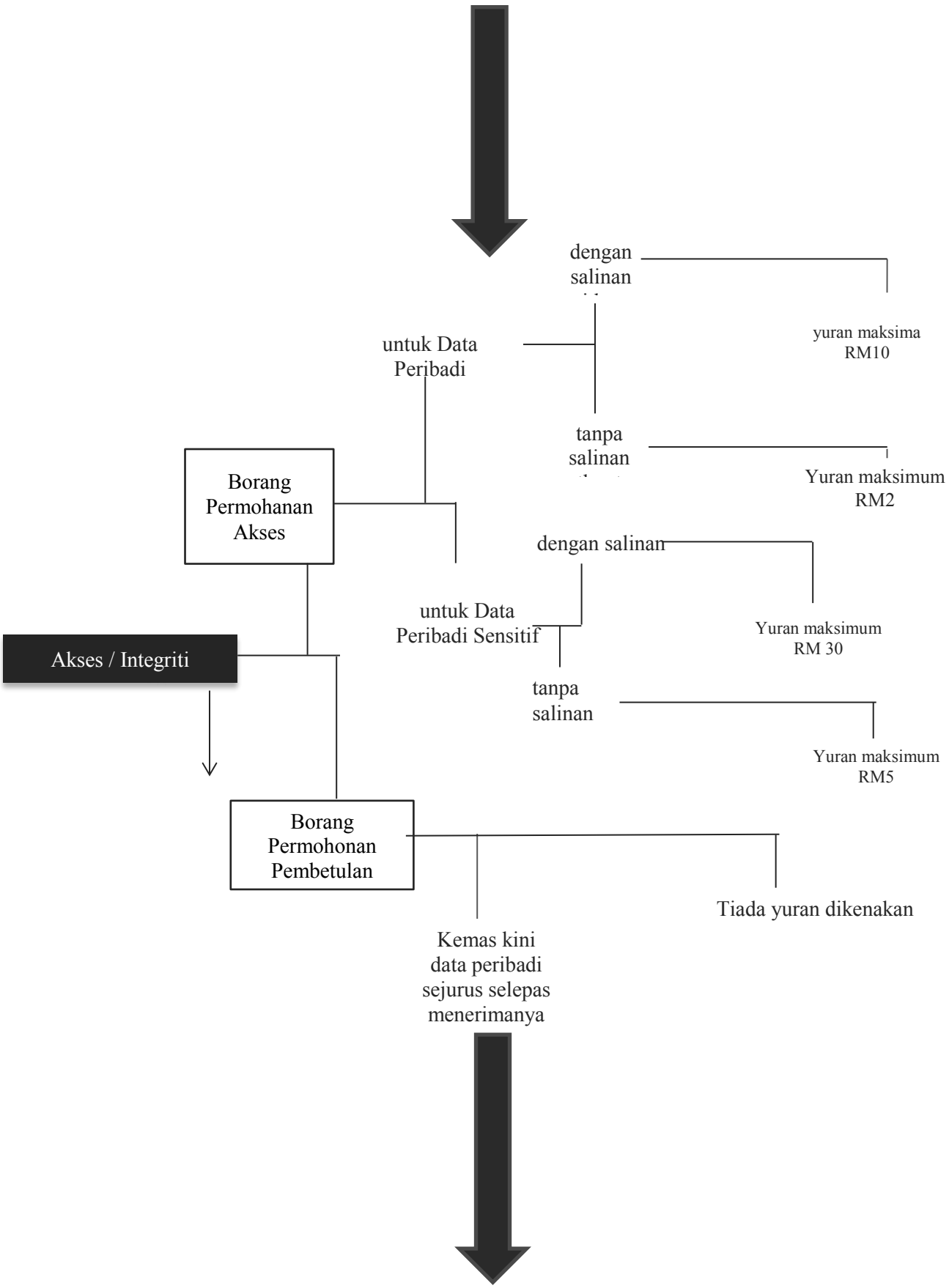
Pihak Ketiga	Berhubung dengan Data Peribadi, bermaksud mana-mana orang selain daripada: (a) Subjek Data; (b) seseorang yang berkaitan dengan Subjek Data; (c) Pengguna Data; (d) Pemproses Data; atau (e) seseorang yang diberikan kuasa secara bertulis oleh Pengguna Data untuk memproses Data Peribadi dibawah kawalan Pengguna Data.
Menulis / Bertulis	Semua manual atau cara elektronik untuk merekod maklumat di dalam bentuk yang boleh disimpan dan dicetak, sama ada dalam manuskrip, menggunakan mesin taip atau komputer, atau menggunakan peranti perhubungan elektronik yang lain.

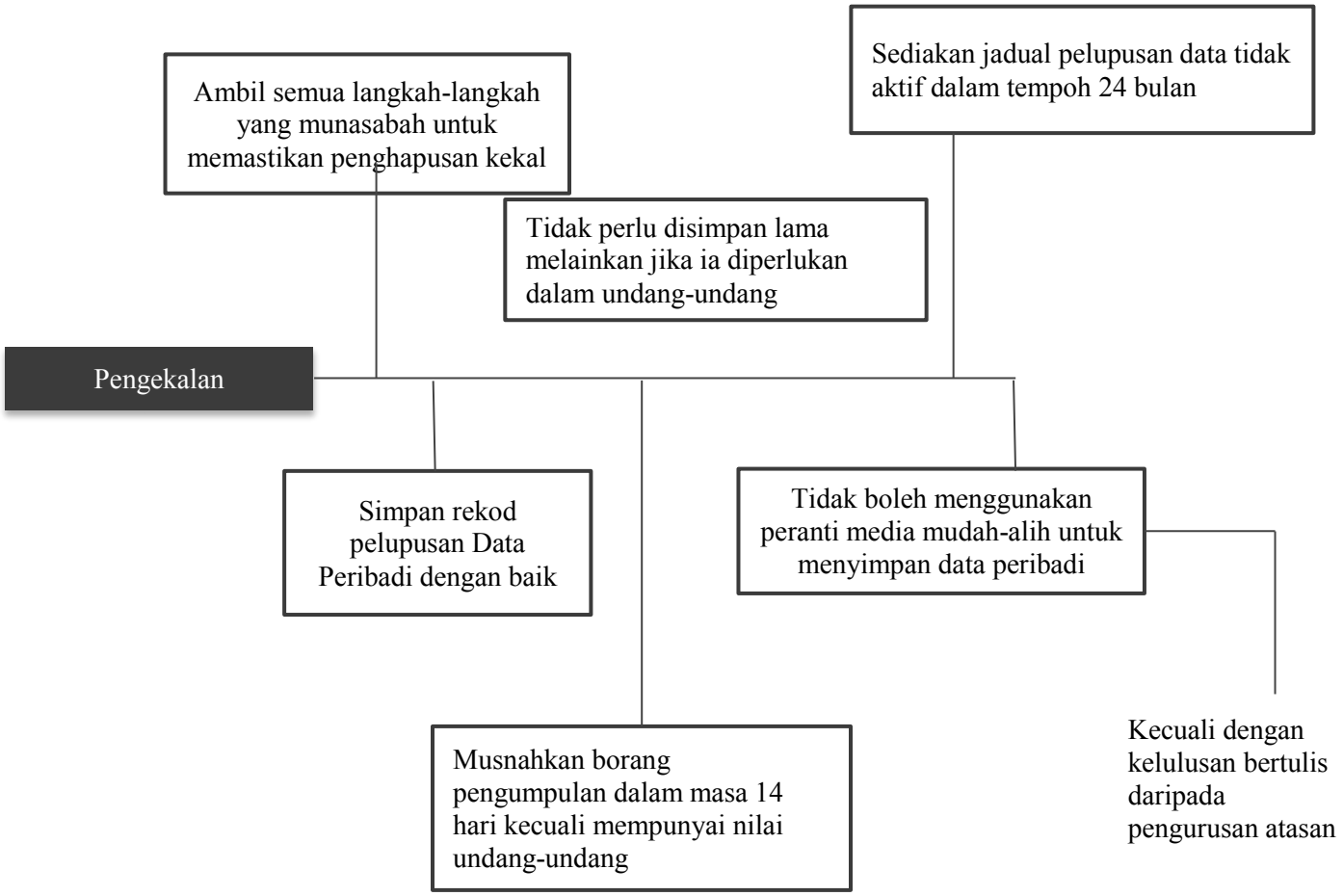
LAMPIRAN 2: ALIRAN DATA




Untuk promosi dan pemasaran
Untuk memberikan perkhidmatan
Untuk tujuan perundangan dan pengawalseliaan
MENGAPA?
Untuk tujuan kewangan
Untuk keselamatan dan kesejahteraan
Untuk siasatan aduan dan pertanyaan
Untuk memudahkan penyediaan penerbangan
Pemberi Perkhidmatan
Affiliate
Penzahiran kepada siapa? (Pihak Ketiga)
Affiliate luar negara


Pengurusan
Tidak boleh dipindahkan melalui peranti mudah-alih dan perkhidmatan penkomputeran awan
Melainkan dengan persetujuan bertulis daripada pihak penguruan atasan
Daftarkan mereka yang boleh akses
Kawal dan hadkan akses berdasarkan keperluan
Keselamatan
Kekalkan rekod akses dan pemindahan
Mengikat pihak ketiga yang terlibat
Mengadakan prosedur prosedur keselamatan fizikal
Pastikan semua kakitangan melindungi kerahsiaan


dengan salinan
yuran maksima RM10
untuk Data Peribadi
tanpa salinan
Yuran maksimum RM2
Borang Permohanan Akses
dengan salinan
untuk Data Peribadi Sensitif
Yuran maksimum RM 30
Akses / Integriti
tanpa salinan
Yuran maksimum RM5
Borang Permohonan Pembetulan
Tiada yuran dikenakan
Kemas kini data peribadi sejurus selepas menerimanya


Pengekalan
Ambil semua langkah-langkah yang munasabah untuk memastikan penghapusan kekal
Sediakan jadual pelupusan data tidak aktif dalam tempoh 24 bulan
Tidak perlu disimpan lama melainkan jika ia diperlukan dalam undang-undang
Simpan rekod pelupusan Data Peribadi dengan baik
Tidak boleh menggunakan peranti media mudah-alih untuk menyimpan data peribadi
Kecuali dengan kelulusan bertulis daripada pengurusan atasan
Musnahkan borang pengumpulan dalam masa 14 hari kecuali mempunyai nilai undang-undang

LAMPRIAN 3: PRINSIP AM

Templat Persetujuan untuk Pengumpulan Data Peribadi Secara Dalam Talian

Templat persetujuan di mana pelanggan perlu bersetuju sebelum melakukan sebarang tempahan.

- *Saya telah membaca dan memahami **[masukkan syarikat penerbangan]** Dasar Privasi **[pautan]** dan bersetuju untuk **[masukkan syarikat penerbangan]** menggunakan maklumat peribadi saya seperti yang telah diterangkan dalam dasar tersebut, termasuk sebarang penzahiran dan pemindahan yang perlu.*

Templat persetujuan untuk pemasaran langsung. Pelanggan mesti menyatakan persetujuan secara jelas untuk menerima pemasaran langsung daripada syarikat penerbangan.

- *Saya ingin menerima komunikasi dan maklumat terkini pada masa akan datang daripada **[masukkan syarikat penerbangan]** dan juga rakan kongsi.*

LAMPIRAN 4: PRINSIP NOTIS DAN PILIHAN

Templat Notis Privasi

1. Pengenalan

[Masukkan nama] (dirujuk sebagai "**Syarikat**" atau "**kami**") adalah komited untuk melindungi Data Peribadi anda dan melindungi privasi anda adalah keutamaan yang tinggi.

Pernyataan Privasi ini menerangkan terma am tentang bagaimana kami mengumpul, menggunakan dan melindungi privasi Data Peribadi anda di bawah Akta Perlindungan Data Peribadi 2010 ("**APDP**").

2. Apakah Data Peribadi yang kami kumpul?

Jenis-jenis Data Peribadi yang kami kumpul secara langsung daripada anda atau daripada pihak ketiga adalah bergantung kepada keadaan semasa pengumpulan dan jenis perkhidmatan yang diminta atau transaksi yang dijalankan. Ia mungkin termasuk (tetapi tidak terhad kepada):
[sila padamkan yang tidak berkenaan]

(a) maklumat peribadi yang dikaitkan dengan seseorang individu, seperti, nama, jantina, tarikh lahir, nombor pasport, nombor kad pengenalan kebangsaan yang dikeluarkan oleh kerajaan lain dan nombor pengenalan peribadi yang lain;
(b) maklumat perhubungan, seperti, alamat, nombor telefon dan alamat e-mel;
(c) maklumat pembayaran, seperti maklumat kad kredit atau kad debit, termasuk nama pemegang kad, nombor kad, alamat bil dan tarikh tamat tempoh;
(d) maklumat perjalanan, seperti maklumat penerbangan, butiran keahlian program kesetiaan, tempat duduk, diet pemakanan atau pilihan perkhidmatan yang lain;
(e) maklumat kesihatan, seperti isu kesihatan yang berkaitan dengan persiapan perjalanan atau rekod kesihatan dan permintaan;
(f) maklumat teknikal, seperti alamat IP; dan
(g) data statistik, seperti jumlah penumpang dan lawatan ke laman *web*.

Jika orang lain yang membuat tempahan bagi pihak anda, anda menerima dan akan memastikan bahawa anda telah memberi kebenaran untuk penzahiran Data Peribadi anda dan persetujuan kepada terma dan syarat Pernyataan Privasi ini. Jika anda membuat tempahan bagi pihak orang lain, anda mewakili dan menjamin bahawa anda telah mendapat persetujuan daripada orang tersebut untuk memberikan Data Peribadi mereka. Sebagai tambahan, jika anda membuat tempahan bagi pihak kanak-kanak (yang berumur

18 tahun ke bawah), sila pastikan bahawa anda berumur lebih daripada 18 tahun, mempunyai kebenaran dan persetujuan mereka untuk menyerahkan Data Peribadi mereka kepada Pengguna Data.

3. <u>Bagaimana kami mengumpul Data Peribadi anda?</u>

Dasar Privasi ini meliputi sebarang Data Peribadi yang diberikan kepada kami:

[sila padamkan yang tidak berkenaan]

(a) bila membuat tempahan dengan kami, daftar masuk untuk penerbangan atau penghantaran barang;
(b) melalui mana-mana laman *web* yang dikendalikan oleh kami atau kontraktor kami;
(c) dibawah mana-mana perjanjian berkontrak atau persetujuan yang lain;
(d) melalui pihak ketiga, seperti agensi pelancongan atau pembekal perkhidmatan kami.

Beberapa cara lain yang mungkin kami mengumpul Data Peribadi termasuk (tetapi tidak terhad kepada):

(a) komunikasi dengan anda melalui telefon, surat, faks dan e-mel;
(b) apabila anda melawat laman *web* kami atau laman *web* salah satu kontraktor kami;
(c) apabila anda berhubung dengan kami secara peribadi;
(d) apabila kami menghubungi anda secara peribadi;
(e) apabila kami mengumpul maklumat tentang anda daripada pihak ketiga;
(f) apabila anda berinteraksi dengan kami melalui media sosial, atau aplikasi interaktif termasuk tetapi tidak terhad kepada Facebook, Twitter, Instagram dll;
(g) daripada sumber awam yang tersedia ada;
(h) perkhidmatan mudah-alih;
(i) saluran-saluran lain termasuk kaunter tiket dan operasi lapangan terbang kami.

4. <u>Bagaimana kami mengumpul Data Peribadi anda daripada laman *web* kami?</u>

Daripada laman *web* kami, kami mengumpul Data Peribadi anda melalui beberapa cara seperti berikut:

(a) <u>Alamat IP</u>

Kami menggunakan alamat IP anda untuk membantu mendiagnosis masalah dengan pelayar kami, dan untuk mentadbir laman *web* kami. Alamat IP tidak akan dipaut kepada maklumat peribadi yang boleh dikenal pasti.

(b) *Cookie*

Cookie adalah elemen data yang boleh dihantar oleh laman *web* kepada pelayar anda, di mana ia boleh disimpan di dalam sistem anda. Kami menggunakan *cookie* di dalam beberapa halaman kami untuk menyimpan pilihan dan merekodkan maklumat sesi anda. Maklumat yang kami kumpul akan digunakan untuk memastikan perkhidmatan istimewa diberikan kepada pengguna kami. Kami berharap anda berasa yakin apabila anda perlu menaip nombor kad kredit anda setiap kali anda membuat pembelian walaupun nombor kad kredit anda tidak akan disimpan atas alasan keselamatan,.

Anda boleh memperbetulkan tetapan pada pelayar anda agar anda akan diberitahu apabila anda menerima *cookie*. Sila rujuk kepada dokumen pelayar anda untuk memeriksa jika *cookie* telah diaktifkan pada komputer anda atau meminta untuk tidak menerima *cookie*. Oleh kerana *cookie* membenarkan anda untuk memanfaatkan beberapa ciri-ciri penting pada laman *web*, kami mencadangkan agar anda menerima *cookie*. Sebagai contoh, jika anda menyekat atau menolak *cookie* kami, anda tidak boleh menempah penerbangan atau menggunakan sebarang produk atau perkhidmatan di laman *web* yang memerlukan anda untuk log masuk.

Adalah penting untuk menghalang akses yang tidak dibenarkan pada kata laluan dan komputer anda. Anda harus log keluar selepas menggunakan komputer yang dikongsi.

Kami juga menggunakan *cookie* untuk mengesan keberkesanan pengiklanan dalam talian. Maklumat ini diuruskan secara rahsia dan tidak akan dikongsi dengan sesiapa yang berada di luar Syarikat melainkan dinyatakan di dalam Dasar Privasi ini. Kami hanya akan menggunakan maklumat ini untuk membuat keputusan yang tepat berhubung dengan pembelian secara pengiklanan dalam talian.

(c) Sistem Tempahan Dalam Talian

Sistem tempahan dalam talian kami terletak di dalam pelayar yang disulitkan (encrypt) maklumat pembelian anda menggunakan Lapisan Soket Selamat. Kami menggunakan semua usaha yang munasabah untuk melindungi Data Peribadi daripada hilang, disalahgunakan dan diubahsuai. Hanya kakitangan dan ejen yang dibenarkan sahaja akan diberi akses kepada Data Peribadi anda. Walau bagaimanapun, anda bertanggungjawab terhadap ID pengguna atau kata laluan anda yang digunakan di dalam laman *web* kami. Anda harus berhati-hati untuk melindunginya.

(d) Borang Maklum Balas Pengguna

Borang Maklum Balas Khidmat Pelanggan kami memerlukan anda untuk memberi maklumat perhubungan (seperti nama anda dan e-mel) agar kami boleh membalas komen anda. Kami menggunakan maklumat perhubungan anda daripada borang pendaftaran untuk menghantar maklumat berkenaan syarikat kami. Maklumat perhubungan anda juga akan digunakan untuk menghubungi anda apabila perlu. Data demografik dan profil juga dikumpulkan di laman *web* kami. Kami menggunakan Data Peribadi anda untuk menyesuaikan pengalaman anda di laman *web* kami dengan menunjukkan kandungan yang kami fikirkan anda mungkin berminat dengan kandungan tersebut mengikut keutamaan anda.

(e) Pengesanan Tapak

Kami menggunakan perisian pengesanan untuk memantau corak trafik pelanggan dan penggunaan tapak untuk membantu kami menghasilkan reka bentuk dan susun atur laman *web*. Perisian ini tidak membolehkan kami untuk mengambil sebarang maklumat peribadi penumpang.

5. Untuk apakah kami menggunakan Data Peribadi anda?

Kami mungkin menggunakan Data Peribadi anda untuk tujuan berikut:

(a) untuk membolehkan kami memberikan perkhidmatan kami dan melaksanakan perkhidmatan kami kepada anda;
(b) untuk memudahkan perjalanan anda (seperti membuat tempahan) dan persiapan penghantaran barang;
(c) untuk pengesahan identiti penumpang dan melaksanakan daftar masuk bagasi;
(d) untuk memberi mesej siap sedia penerbangan;
(e) untuk memudahkan daftar masuk internet;
(f) untuk memproses sebarang transaksi komersial (seperti jualan dalam penerbangan);
(g) untuk memudahkan penyertaan anda dalam program kesetiaan kami atau pihak ketiga;
(h) untuk melindungi keselamatan dan kesejahteraan anda dan pelanggan yang lain;
(i) untuk menyiasat dan bertindak balas tentang tuntutan dan pertanyaan daripada anda;
(j) untuk mengingatkan anda untuk melengkapkan tempahan anda dan / atau menawarkan bantuan kami (contoh seperti, kegagalan melengkapkan kerana kesulitan teknikal). Ini adalah perkhidmatan pilihan. Anda boleh memilih untuk tidak menerima e-mel ini pada bila-bila masa dengan mengikuti pautan di bahagian bawah e-mel tersebut;

(k) untuk menyediakan perkhidmatan penyediaan katering dalam penerbangan dan perkhidmatan lain yang paling sesuai mengikut keutamaan dan keperluan anda;

(l) untuk tujuan kewangan seperti pengesahan, perakaunan, bil dan audit berkenaan kredit atau pembayaran kad yang lain;

(m) untuk tujuan pembangunan perniagaan seperti analisis statistik pemasaran, percubaan sistem, penyelenggaraan dan pembangunan, kaji selidik pelanggan, berhubung dengan pelanggan tentang pengubahsuaian penerbangan, atau untuk membantu kami berurusan dengan anda di masa hadapan, sebagai contoh untuk mengenal pasti keperluan dan pilihan anda;

(n) untuk mematuhi sebarang keperluan undang-undang atau peraturan; dan / atau

(o) untuk tujuan sampingan yang lain untuk sebarang tujuan seperti yang dinyatakan di atas.

("**Tujuan Utama**")

(p) untuk mengkomunikasikan promosi, tawaran, perkhidmatan dan maklumat tentang produk dan aktiviti, tawaran untuk menaik taraf atau pemberitahuan lain yang berkaitan dengan tempahan anda;

(q) pemasaran dan berkomunikasi dengan anda berhubung dengan produk dan perkhidmatan yang ditawarkan oleh kami dan rakan perkhidmatan kami serta ejen yang dilantik oleh kami; dan / atau

(r) untuk semua tujuan sampingan yang lain untuk sebarang tujuan seperti yang dinyatakan di atas.

("**Tujuan Sampingan**")

(secara kolektif, "**Tujuan**")

6. <u>Mengakses / Menghadkan / Memperbetulkan / Mengemas Kini Data Peribadi anda</u>

Anda boleh memohon untuk mendapatkan maklumat Data Peribadi anda, menghadkan pemprosesan Data Peribadi anda dan juga mengemas kini atau membuat pindaan kepada Data Peribadi anda seperti di bawah:

(a) untuk pelanggan berdaftar dalam talian, anda boleh log masuk ke akaun dalam talian anda dan mengemas kini Data Peribadi anda; atau

(b) untuk setiap pelanggan lain, anda boleh mengemukakan permintaan anda kepada mereka yang boleh dihubungi seperti yang terperinci di bawah klausa 13.

Sila ambil perhatian bahawa bergantung kepada maklumat yang diminta, yuran nominal mungkin akan dikenakan. Kami akan berusaha untuk memberikan maklumat kepada anda dengan secepat mungkin selagi praktikal. Walau bagaimanapun, kami juga berhak untuk mengesahkan semua permintaan bagi memastikan kesahihan permintaan tersebut. Kami boleh menolak untuk mematuhi permintaan akses data di dalam

keadaan seperti yang diperuntukkan oleh undang-undang (di bawah seksyen 32 APDP). Sekiranya kami tidak dapat memenuhi permintaan anda, kami akan memberitahu anda sebab-sebabnya.

7. <u>Menarik balik Persetujuan</u>

Sila ambil perhatian bahawa adalah wajib bagi Syarikat untuk memproses Data Peribadi anda untuk Tujuan Utama seperti yang telah dinyatakan diatas, di mana tanpanya kami tidak boleh mambuat pengaturan perjalanan untuk anda. Sekiranya kami tidak mendapat persetujuan anda untuk memproses Data Peribadi anda untuk Tujuan Sampingan, kami tidak boleh memaklumkan kepada anda tentang masa depan, produk dan perkhidmatan baru dan / atau sebarang penambahbaikan kami.

Walau bagaimanapun, anda boleh berhenti menerima aktiviti promosi dengan:

(a) berhenti melanggan daripada senarai mel;
(b) menyunting tetapan akaun yang berkaitan untuk berhenti melanggan; atau
(c) menghantar permintaan ke ***[masukkan alamat e-mel]***

8. <u>Kepada siapa kami menzahirkan Data Peribadi anda?</u>

Kami tidak akan memperdagangkan atau menjual Data Peribadi anda kepada pihak ketiga. Data Peribadi anda hanya akan dizahirkan atau dipindahkan kepada pihak ketiga seperti yang berikut yang mungkin berada di dalam atau di luar Malaysia untuk memenuhi tujuan:

[sila padam yang tidak berkaitan]

(a) pembekal perkhidmatan perjalanan dan pengangkutan barang kami atau perniagaan yang berkaitan dengan perjalanan;
(b) rakan kongsi syarikat penerbangan dan syarikat penerbangan lain;
(c) pihak berkuasa lapangan terbang;
(d) sekutu dan anak syarikat kami yang lain di mana ia adalah perlu untuk memudahkan perjalanan anda;
(e) pembekal pengesahan kad kredit;
(f) gudang data;
(g) pembekal perkhidmatan teknologi maklumat;
(h) penganalisis data dan / atau agensi pemasaran;
(i) pihak ketiga yang lain untuk memproses transaksi komersial anda;

(j) badan perundangan yang dibenarkan atau dikehendaki oleh undang-undang supaya mematuhi waran atau sepina yang dikeluarkan oleh mahkamah yang mempunyai bidang kuasa kompeten;
(k) kastam, imigresen, atau pihak berkuasa pengawalseliaan yang berkenaan dengan anda; dan / atau
(l) kakitangan keselamatan dan sekuriti.

Di samping itu, data peribadi anda mungkin boleh dizahirkan atau dipindahkan kepada mana-mana pemegang hak sebenar, penerima atau pemeroleh Syarikat (di dalam atau di luar Malaysia) (termasuk sekutu dan anak syarikat kami) atau perniagaan, aset atau syarikat kumpulan kami, atau berkaitan dengan sebarang penstrukturan semula syarikat termasuk penstrukturan semula perniagaan, aset dan / atau tanggungan kami.

Kami akan mengambil langkah-langkah praktikal untuk memastikan bahawa kakitangan, pegawai, ejen, perunding, kontraktor dan pihak ketiga mereka yang disebutkan di atas yang terlibat di dalam pengumpulan, penggunaan dan penzahiran Data Peribadi anda akan mematuhi syarat-syarat Pernyataan Privasi ini.

9. <u>Bagaimana Data Peribadi disimpan?</u>

Kami akan menyimpan Data Peribadi di negara di mana kami berpangkalan iaitu Malaysia. Walau bagaimanapun, Syarikat mungkin mempunyai sandaran dan pelayar penyimpanan yang terletak di luar negara. Di samping itu, Syarikat akan memastikan penyimpanan dengan cara berikut dengan mematuhi langkah keselamatan yang minimum seperti yang ditetapkan di bawah APDP, peraturan dan standardnya:

(a) Mendaftarkan semua orang yang diberikan akses;
(b) mengawal dan menghadkan akses berdasarkan keperluan;
(c) mengekalkan rekod yang mencukupi untuk mengakses dan pemindahkan Data Peribadi;
(d) memastikan semua kakitangan Syarikat melindungi kerahsiaan;
(e) menjalankan program kesedaran kepada semua kakitangan (jika perlu) tentang tangungjawab untuk melindungi Data Peribadi;
(f) mewujudkan prosedur keselamatan fizikal;
(g) mengikat pihak ketiga yang terlibat dalam pemprosesan Data Peribadi; dan
(h) tidak menggunakan peranti yang boleh ditanggal dan perkhidmatan pengkomputeran awan untuk memindahkan atau menyimpan Data Peribadi kecuali dengan persetujuan bertulis daripada pengurusan atasan Syarikat

10. Berapa lamakah kami menyimpan Data Peribadi anda?

Kami tidak akan menyimpan Data Peribadi anda lebih lama daripada yang diperlukan untuk memenuhi tujuan. Walau bagaimanapun, Data Peribadi yang berkenaan mungkin disimpan tertakluk kepada syarat di bawah:

(a) sebagaimana dan apabila dikehendaki di bawah undang-undang; atau
(b) di mana tindakan undang-undang telah berlaku dan belum selesai.

Syarikat akan mengambil langkah-langkah yang munasabah untuk memastikan bahawa semua Data Peribadi dimusnahkan atau dipadam secara kekal apabila dia tidak lagi diperlukan untuk Tujuan dan menyediakan jadual pelupusan untuk data yang tidak aktif selama tempoh 24 bulan.

11. Perubahan kepada Pernyataan Privasi

Sila ambil perhatian bahawa Penyataan Privasi ini boleh dipinda dari semasa ke semasa mengikut undang-undang dan peraturan yang berkenaan dan variasi tersebut mungkin terpakai kepada anda.

Versi terkini Pernyataan Privasi ini disediakan kepada semua pelanggan.Sila lawat laman *web* kami dari semasa ke semasa untuk maklumat terkini tentang Pernyataan Privasi kami.

12. Pautan kepada laman *web* pihak ketiga

Kami mungkin pautkan laman *web* ini dan / atau permohonan kepada laman *web* syarikat atau organisasi lain (secara kolektif, "Laman *Web* Pihak Ketiga"). Notis Privasi ini tidak terpakai kepada Laman *Web* Pihak Ketiga kerana laman tersebut adalah di luar kawalan kami. Jika anda mengakses Laman *web* Pihak Ketiga dengan menggunakan pautan yang diberikan, penggendali laman ini mungkin akan mengumpul maklumat peribadi anda. Sila pastikan bahawa anda berpuas hati dengan pernyataan privasi Laman *Web* Pihak Ketiga tersebut sebelum anda menyerahkan sebarang maklumat peribadi. Kami mencuba sejauh mana yang boleh untuk memastikan bahawa semua laman *web* pihak ketiga mempunyai langkah-langkah untuk melindungi maklumat peribadi anda, tetapi kami tidak boleh bertanggungjawab secara sah atau sebaliknya untuk sebarang aktiviti, dasar privasi atau tahap pematuhan privasi Laman *Web* Pihak Ketiga tersebut.

13. Maklumat Perhubungan

Sekiranya anda masih mempunyai pertanyaan atau aduan berhubung dengan pengendalian Data Peribadi anda atau Dasar Privasi atau ingin mengakses, mengemaskini atau meminda Data Peribadi anda seperti yang dinyatakan di atas pada Klausa 6, sila hubungi kami melalui butiran seperti yang dihuraikan di bawah:

Jawatan : ***[masukkan]***

No. telefon : ***[masukkan]***

No. Faks (jika ada) : ***[masukkan]***

Alamat E-mel (jika ada) : ***[masukkan]***

Anda juga boleh memasukkan maklumat lain yang berkenaan, contoh alamat pejabat.

LAMPIRAN 5: DATA PERIBADI YANG DIZAHIRKAN ATAU DITERIMA DARIPADA PIHAK KETIGA

Senarai Penzahiran

(Lampiran in tidak bertujuan secara menyeluruh tetapi mungkin dipinda dari semasa ke semasa seperti yang diluluskan oleh Pesuruhjaya Perlindungan Data Peribadi)

NO.	PIHAK KETIGA
1.	Instutusi kewangan, peniaga, Persatuan Perkhidmatan VISA Antarabangsa, Perbadanan Antarabangsa MasterCard dan persatuan kad yang lain (berkaitan dengan isu kad kredit kepada Subjek Data) untuk tujuan pembayaran tiket penerbangan atau perkhidmatan lain daripada Pengguna Data
2.	Pengusaha pos yang menyediakan perkhidmatan pos kepada Pengguna Data
3.	Pembekal telekomunikasi yang menyediakan perkhidmatan telekomunkasi kepada Pengguna Data
4.	Pembekal perkhidmatan yang membantu Pengguna Data dalam pemprosesan perkhidmatan yang diminta oleh Pengguna Data: (a) Pembekal perjalanan dan penghantaran barang atau perniagaan yang berkaitan dengan perjalanan (b) Rakan syarikat penerbangan dan syarikat penerbangan lain (c) Pihak berkuasa lapangan terbang (d) Sekutu atau anak syarikat Pengguna Data di mana perlu untuk memudahkan perjalanan Subjek Data
5.	Ejen / kontraktor / perunding / pembekal / juruaudit luaran / kaunselor / pemproses data yang dilantik oleh Pengguna Data (a) Gudang data (b) Pembekal perkhidmatan teknologi maklumat (c) Agensi penganalisis data (d) Agensi pemasaran
6.	Badan-badan yang diluluskan di mana sumbangan kakitangan diberikan: (a) Pertubuhan Keselamatan Sosial (PERKESO) (b) Baitulmal (c) Pusat Zakat (d) Lembaga Tabung Haji

	(e) Yayasan Pembangunan Ekonomi Islam Malaysia (YaPEIM) (f) Kumpulan Wang Simpanan Pekerja (KWSP) (g) Koperasi Wawasan Pekerja-pekerja Berhad (KOWAJA) (h) Penanggung insuransn/ Broker
7.	Ahli keluarga rapat Subjek Data: (a) Bapa (b) Emak (c) Suami (d) Isteri (e) Adik-beradik
8.	Permintaan maklumat oleh Kerajaan Persekutuan atau Kerajaan Negeri daripada Pengguna Data. Berikut adalah contoh yang dinyatakan, oleh itu ia termasuk tetapi tidak terhad kepada seperti di bawah: (a) Jabatan Pembangunan Islam Malaysia (b) Jabatan Bantuan Guaman Malaysia (c) Jabatan Statistik Malaysia (d) Jabatan Immigresen Malaysia (e) Lembaga Hasil Dalam Negeri Malaysia (perkara yang berkaitan dengan cukai pendapatan) (f) Majlis Amanah Rakyat di bawah Kementerian Pembangunan Luar Bandar dan Wilayah (g) Suruhanjaya Pencegahan Rasuah Malaysia (h) Jabatan Insolvensi Malaysia (i) Kementerian Perdagangan Dalam Negeri, Koperasi dan Kepenggunaan (j) Kementerian Kewangan Malaysia (k) Kementerian Kesihatan Malaysia (l) Kementerian Sumber Manusia Malaysia (m) Jabatan Kastam Diraja Malaysia (n) Polis Diraja Malaysia (o) Suruhanjaya Sekuriti (p) Jabatan Kehakiman Syariah Malaysia

	(q) Jabatan Agama (r) Majlis Perbandaran (s) Majlis Daerah (t) Majlis Agama Islam Negeri (u) Perbadanan Tabung Pendidikan Tinggi Nasional (PTPTN) (v) Perbadanan Pembangunan Filem Nasional Malaysia (FINAS)
9.	Anak syarikat milik penuh Pengguna Data
10.	Doktor / klinik / hospital / farmasi panel yang dilantik oleh Pengguna Data
11.	Kakitangan keselamatan dan sekuriti Pengguna Data
12.	Mana-mana orang yang berkaitan dengan penguatkuasaan atau pemeliharaan hak Pengguna Data di bawah perjanjian yang telah dimeterai dengan Pengguna Data
13.	Syarikat atau organisai yang membantu Pengguna Data dalam memberikan perkhidmatan bernilai seperti yang diminta oleh Subjek Data
14.	Mana-mana orang yang diberitahu dan diberikan kuasa oleh Subjek Data
15.	Mana-mana orang yang berniat untuk menyelesaikan hutang tertunggak yang berkaitan dengan perkhidmatan Pengguna Data kepada Subjek Data
16.	Di mana Pengguna Data dikehendaki atau dibenarkan oleh mana-mana perintah mahkamah / tribunal atau pihak berkuasa sama ada kerajaan atau kerajaan kuasi dengan bidang kuasa ke atas Pengguna Data
17.	Mana-mana orang / syarikat yang dilantik oleh Pengguna Data untuk memulihkan hutang tertunggak yang dialami Pengguna Data
18.	Penasihat Pengguna Data (termasuk tetapi tidak terhad kepada akauntan, juruaudit, peguam atau penasihat profesional yang lain) seperti yang dibenarkan oleh Pengguna Data
19.	Pihak yang diperlukan atau dibenarkan oleh undang-undang untuk Pengguna Data
20.	Pihak yang Pengguna Data boleh memindahkan hak dan tanggungjawab menurut perjanjian yang disahkan dengan Subjek Data
21.	Pemegang hak sebenar, penerima atau pemeroleh (di dalam atau di luar Malaysia) Pengguna Data berkenaan perniagaan, aset atau syarikat kumpulan atau berkaitan dengan sebarang penstrukturan semula

Data Peribadi yang diterima daripada Pihak Ketiga

[Pihak Ketiga] harus mematuhi sepenuhnya peruntukan Akta Perlindungan Data Peribadi dan sebarang peraturan, panduan pengawalseliaan, perintah, standard, arahan, kod tataamalan atau instrumen pengawalseliaan lain yang serupa dikeluarkan menurutnya ("Akta") yang terpakai bagi pemprosesan data peribadi seperti yang ditakrifkan di dalam Akta dan khususnya, bahawa semua persetujuan telah diperolehi daripada individu yang mana data peribadinya boleh dizahirkan kepada Syarikat Penerbangan menurut Perjanjian ("Penzahiran Data") berkenaan dengan penzahiran dan pemprosesan oleh Syarikat Penerbangan dan bahawa [pihak ketiga] akan sentiasa menyediakan kepada Syarikat Penerbangan dengan Penzahiran Data yang telah dikemaskini.

[Pihak Ketiga] harus melindungi Syarikat Penerbangan terhadap semua prosiding, kos, perbelanjaan, tanggungan atau ganti rugi yang terjadi akibat [pihak ketiga] gagal mematuhi Akta berkenaan dengan sebarang Penzahiran Data. Pembetulan yang tersedia ada dalam klausa ini kepada Syarikat Penerbangan adalah tidak menjejaskan dan sebagai tambahan kepada sebarang jaminan, ganti rugi, remedi atau hak-hak lain yang disediakan oleh undang-undang atau Perjanjian.

Penzahiran Data Peribadi kepada Pihak Ketiga

1. Pemproses Data harus mematuhi Akta Perlindungan Data Peribadi dan sebarang peraturan, panduan pengawalseliaan, perintah, standard, arahan, kod tataamalan atau instrumen pengawalseliaan lain yang serupa dikeluarkan mengikut pemprosesan Data Peribadi (secara kolektif, "Undang-undang Privasi").
2. Pemproses Data harus memproses data peribadi hanya bagi pihak dan untuk manfaat Syarikat Penerbangan, untuk tujuan pemprosesan data peribadi yang berkaitan dengan Perjanjian, dan menjalankan tanggungjawab mereka menurut Perjanjian dan arahan bertulis Syarikat Penerbangan.
3. Syarikat Penerbangan harus mempunyai kuasa yang eksklusif untuk menentukan tujuan dan cara pemprosesan data peribadi di bawah Perjanjian ini.
4. Pemproses Data dan kakitangan, ejen, perunding atau kontraktor mereka (“Kakitangan”) harus memegang kerahsiaan tentang sebarang atau semua Data Peribadi.
5. Pemproses Data harus menghadkan akses data peribadi kepada kakitangannya yang mempunyai keperluan untuk mengetahui data peribadi sebagai syarat untuk prestasi perkhidmatan Pemproses Data untuk atau bagi pihak Syarikat Penerbangan.

6. Di mana Pemproses Data berkongsi, memindahkan, mendedahkan atau memberi akses sebarang data peribadi kepada mana-mana pihak ketiga atau sebarang kontrak berkenaan hak atau tanggungjawab yang melibatkan Data Peribadi, Pemproses Data harus membuat perjanjian bertulis dengan setiap kontraktor atau pihak ketiga dengan mengenakan tanggungjawab keatas kontraktor atau pihak ketiga seperti yang sama dengan yang dikenakan pada Pemproses Data di bawah Perjanjian ini.
7. Pemproses Data hanya perlu mengekalkan kontraktor yang boleh diharapkan oleh Pemproses Data untuk melindungi privasi, kerahsiaan dan keselamatan Data Peribadi.
8. Pemproses Data tidak harus memindahkan data peribadi ke luar Malaysia tanpa persetujuan bertulis yang jelas daripada Syarikat Penerbangan.
9. Pemproses Data harus membalas sebarang permintaan berkaitan dengan data peribadi yang diterima oleh Syarikat Penerbangan daripada pelanggan, pengguna, kakitangan atau lain-lain menurut arahan syarikat penerbangan. Pemproses Data harus bekerjasama dengan syarikat penerbangan sekiranya seseorang individu meminta akses kepada data peribadinya untuk sebarang sebab.
10. Pemproses Data harus memberitahu Syarikat Penerbangan dengan serta-merta secara bertulis tentang sebarang sepina atau perintah kehakiman atau pentadbiran lain oleh pihak berkuasa kerajaan atau prosiding mencari akses atau penzahiran data peribadi. Syarikat Penerbangan mempunyai hak untuk mempertahankan tindakan sedemikian sebagai pengganti dan bagi pihak Pemproses Data. Syarikat Penerbangan boleh memilih untuk mencari perintah perlindungan. Pemproses Data harus bekerjasama dengan Syarikat Penerbangan secara munasabah untuk mempertahankannya.
11. Pemproses Data harus mengekalkan perlindungan yang munasabah dan langkah-langkah keselamatan lain yang diwujudkan untuk (i) memastikan keselamatan dan kerahsiaan data peribadi; (ii) melindungi daripada sebarang ancaman atau bahaya yang dijangkakan kepada keselamatan dan integriti data peribadi; dan (iii) melindungi daripada sebarang insiden yang sebenar atau yang disyaki berkenaan pemprosesan, kehilangan, penggunaan, penzahiran atau pengambilalihan atau akses yang tidak dibenarkan kepada sebarang data peribadi **("Insiden Sekuriti Maklumat")**.
12. Pemproses Data harus memaklumkan dengan segera secara bertulis kepada Syarikat Penerbangan tentang sebarang Insiden Sekuriti Maklumat yang mana Pemproses Data menyedarinya, tetapi tidak lebih daripada 24 jam selepas mereka menyedari tentang Insiden Sekuriti Maklumat. Notis tersebut harus diringkaskan dengan terperinci akan kesannya pada Syarikat Penerbangan, jika diketahui, Insiden Sekuriti Maklumat dan tindakan pembetulan yang diambil atau akan diambil oleh Pemproses Data. Pemproses Data harus mengambil segala tindakan pembetulan yang perlu dan dinasihati dengan segera, dan harus bekerjasama sepenuhnya dengan Syarikat Penerbangan di dalam segala usaha yang munasabah dan sah untuk mencegah, mengurangkan atau memperbetulkan Insiden Sekuriti Maklumat tersebut. Kandungan tentang sebarang pemfailan, komunikasi, notis, siaran akhbar atau laporan yang

berkaitan dengan sebarang Insiden Sekuriti Maklumat mesti diluluskan oleh Syarikat Penerbangan sebelum sebarang penerbitan atau perhubungannya.

13. Apabila tamat tempoh atau penamatan Perjanjian sebelum tempoh, atau awal seperti permintaan syarikat penerbangan, Pemproses Data harus dengan segera kembali kepada Syarikat Penerbangan atau penerima, atau atas permintaan Syarikat Penerbangan, memusnahkan atau menjadikan tidak boleh dibaca atau tidak dapat difahami dengan selamat jika pengembalian tidak munasabah untuk dilaksanakan atau tidak wajar kepada Syarikat Penerbangan (yang mana keputusan harus berdasarkan kepada kenyataan bertulis Syarikat Penerbangan), setiap media asal dan salinan yang mengandungi semua data peribadi dalam pemilikan, penjagaan atau pengawalan Pemproses Data. Sekiranya undang-undang yang berkenaan tidak membenarkan Pemproses Data untuk mematuhi penghantaran atau pemusnahan data peribadi, Pemproses Data menjamin bahawa ia akan memastikan kerahsiaan data peribadi dan ia tidak harus menggunakan atau menzahirkan sebarang data peribadi selepas tamat Perjanjian.

14. Syarikat Penerbangan mempunyai hak untuk memantau pematuhan Pemproses Data dengan syarat-syarat Perjanjian ini. Semasa waktu perniagaan biasa, dan tanpa notis terlebih dahulu, Syarikat Penerbangan atau wakilnya yang sah boleh memeriksa kemudahan dan peralatan Pemproses Data, dan sebarang maklumat atau bahan pemilikan, di dalam jagaan atau kawalan Pemproses Data, yang berkaitan dengan sebarang cara untuk tanggungjawab Pemproses Data di bawah Perjanjian ini. Pemeriksaan yang dijalankan menurut Perjanjian ini tidak boleh mengganggu urusan biasa perniagaan Pemproses Data. Pemproses Data harus bekerjasama sepenuhnya dengan sebarang pemeriksaan yang dijalankan oleh Syarikat Penerbangan.

15. Pemproses Data harus menangani segera dan sewajarnya dengan sebarang pertanyaan daripada Syarikat Penerbangan yang berkaitan dengan pemprosesan data peribadi yang tertakluk kepada perjanjian.

16. Pemproses Data bersetuju untuk melindungi dan memegang Syarikat Penerbangan yang tidak berbahaya dan pegawai, kakitangan, pengarah dan ejen daripada, dan pada pilihan Syarikat Penerbangan untuk pertahanan terhadap sebarang dan semua tuntutan, kerugian, tanggungan, kos dan perbelanjaan, termasuk tuntutan pihak ketiga, yuran peguam yang munasabah, yuran perunding dan kos mahkamah (secara kolektif, "Tuntutan"), setakat mana Tuntutan tersebut timbul, atau mungkin dengan apa-apa cara yang berkaitan dengan (i) sebarang pelanggaran Perjanjian ini; (ii) kecuaian, kecuaian kasar, kepercayaan tidak baik, atau salah laku yang disengajakan oleh Pemproses Data atau Kakitangannya berkaitan dengan tanggungjawab yang dinyatakan di dalam Perjanjian ini; (iii) Penggunaan Pemproses Data daripada sebarang kontraktor yang memberikan perkhidmatan yang berhubung dengan atau berkaitan dengan prestasi Pemproses Data di bawah Perjanjian ini; atau (iv)

sebarang Insiden Sekuriti Maklumat yang melibatkan data peribadi dalam pemilikan, penjagaan atau pengawalan Pemproses Data, atau yang mana Pemproses Data bertanggungjawab.

LAMPIRAN 6: BORANG PERMINTAAN AKSES DATA/ BORANG PERMINTAAN PEMBETULAN DATA

BORANG PERMINTAAN PEMBETULAN DATA PERIBADI

Untuk tujuan borang ini, Subjek Data/Orang yang Berkenaan (seperti yang ditakrifkan di bawah Akta Perlindungan Data Peribadi 2010) mesti menyediakan salinan kad pengenalan (KP) atau pasport, surat kebenaran oleh Subjek Data (di mana anda meminta bagi pihak Subjek Data) dan dokumen sokongan yang berkaitan seperti yang kami kehendaki. Sila ambil perhatian bahawa, kami mungkin tidak boleh memproses permintaan anda sekiranya data peribadi yang diberikan tidak tepat, tidak lengkap, mengelirukan atau tidak dikemas kini. Permintaan untuk memperbetulkan data peribadi adalah tertakluk kepada keperluan di bawah Akta Perlindungan Data Peribadi 2010.

BAHAGIAN 1: UNTUK DIISI OLEH SUBJEK DATA	
Nama Penuh seperti di dalam KP	
KP Baru (Lampirkan salinan)	
*Telefon Rumah	
*Telefon Pejabat	
Telefon Bimbit	
BAHAGIAN 2: UNTUK DIISI OLEH INDIVIDU YANG BERKENAAN	
A : Maklumat Subjek Data	
Nama Penuh seperti di dalam KP	
KP Baru (Lampirkan salinan)	
B : Maklumat Individu yang Berkenaan	
Nama Penuh seperti di dalam KP	
KP Baru	
Alamat	
*Telefon Rumah	
*Telefon Pejabat	
Telefon Bimbit	

**Maklumat yang tidak wajib*

PEMBETULAN DATA PERIBADI SUBJEK DATA

Sila berikan keterangan tentang data peribadi yang hendak diperbetulkan.	
1.1 1.2 1.3	
Pengakuan oleh Subjek Data Saya,…… ……..... dengan ini mengesahkan bahawa maklumat yang diberikan di dalam borang ini dan sebarang dokumen yang disertakan adalah benar dan tepat. Tandatangan:…… Tarikh:…….	Pengakuan oleh Individu yang Berkenaan Saya,……... ……..... dengan ini mengesahkan bahawa maklumat yang diberikan di dalam borang ini dan sebarang dokumen yang disertakan adalah benar dan tepat. Saya, dengan ini bersetuju bahawa anda boleh menghubungi Subjek Data untuk mengesahkan identiti saya. Tandatangan:…… Tarikh:……

Nota: Jika GST dikenakan ke atas yuran, Subjek Data akan membayar semua GST.

****

UNTUK KEGUNAAN RASMI SAHAJA
[Masukkan nama] meluluskan / menolak (tandakan yang bersesuaian) permintaan ini dibuat pada ***[tarikh permohonan]*** di ***[lokasi cawangan]***. Sebab-sebab penolakan: ☐ tidak dapat mengesahkan identiti peminta;

☐ tidak dapat mengesahkan bahawa peminta telah diberi kuasa untuk mewakili bagi pihak subjek data;

☐ tidak dapat mengesahkan bahawa data peribadi tersebut adalah tidak tepat, tidak lengkap, mengelirukan atau tidak terkini;

☐ tidak dapat mengesahkan bahawa pembetulan tersebut adalah tepat, lengkap, tidak mengelirukan dan terkini; atau

☐ sebab-sebab lain yang dibenarkan di bawah Akta Pelindungan Data Peribadi Malaysia :_____

_____

1.4

1.5

Nama Kakitangan: Tandatangan dan tarikh:

1.6
1.7

_____ _____

1.8

BORANG PERMINTAAN AKSES DATA PERIBADI

Untuk tujuan borang ini, Subjek Data/Orang yang Berkenaan (seperti yang ditakrifkan di bawah Akta Perlindungan Data Peribadi 2010) mesti menyediakan salinan kad pengenalan (KP) atau pasport, surat kebenaran oleh Subjek Data dan dokumen sokongan yang berkaitan seperti yang kami kehendaki. Sila ambil perhatian bahawa kami mungkin tidak boleh memproses permintaan anda sekiranya data peribadi yang diberikan adalah tidak tepat, tidak lengkap, mengelirukan atau tidak terkini. Permintaan untuk mengakses data peribadi adalah tertakluk kepada yuran dan juga keperluan di bawah Akta Perlindungan Data Peribadi 2010.

BAHAGIAN 1 : UNTUK DIISI OLEH SUBJEK DATA	
Nama Penuh seperti di dalam KP	
KP Baru (Lampirkan salinan)	
*Telefon Rumah	
*Telefon Pejabat	
Telefon Bimbit	
BAHAGIAN 2:UNTUK DIISI OLEH INDIVIDU YANG BERKENAAN	
A : Maklumat Subjek Data	
Nama Penuh seperti di dalam KP	
KP Baru (Lampirkan salinan)	
B : Maklumat Individu yang Berkenaan	
Nama Penuh seperti di dalam KP	
KP Baru (Lampirkan salinan)	
Alamat	
*Telefon Rumah	
*Telefon Pejabat	
Telefon Bimbit	
**Maklumat yang tidah wajib*	

AKSES KEPADA DATA PERIBADI SUBJEK DATA

Sila berikan keterangan tentang Data Peribadi yang hendak diakses

Adakah anda memerlukan salinan Data Peribadi? (Sila tandakan (x) di dalam kotak yang relevan)

☐Ya

Perkara	Keterangan	Yuran (RM)
☐ (a)	Data Peribadi	10
☐ (b)	Data Peribadi Sensitif	30

☐Tidak

Perkara	Keterangan	Yuran (RM)
☐ (a)	Data Peribadi	2
☐ (b)	Data Peribadi Sensitif	5

Pengakuan oleh Subjek Data	Pengakuan oleh Individu yang berkenaan
Saya,…….. dengan ini mengesahkan bahawa maklumat yang diberikan di dalam borang ini dan sebarang dokumen yang disertakan adalah benar dan tepat. Tandatangan:…… Tarikh:…….	Saya,…….. dengan ini mengesahkan bahawa maklumat yang diberikan di dalam borang ini dan sebarang dokumen yang disertakan adalah benar dan tepat. Saya, dengan ini bersetuju bahawa anda boleh menghubungi Subjek Data untuk mengesahkan identiti saya. Tandatangan:…… Tarikh:……

Nota: Jika GST dikenakan keatas Yuran, Subjek Data akan membayar semua GST.

****

UNTUK KEGUNAAN RASMI SAHAJA

_***[Masukkan nama]*** meluluskan / menolak (tandakan yang bersesuaian) permintaan ini yang dibuat pada ***[tarikh permintaan]*** di ***[lokasi cawangan]***.

Sebab-sebab penolakan:

☐ tidak dapat mengesahkan identiti peminta;

☐ tidak dapat mengesahkan bahawa peminta telah diberi kuasa untuk mewakili bagi pihak subjek data;

☐ tidak dibekalkan dengan maklumat yang munasabah untuk mencari data peribadi yang berkaitan dengan permintaan akses data;

☐ beban atau perbelanjaan untuk memberi akses adalah tidak sesuai dengan risiko privasi Data Peribadi yang berkaitan dengan data peribadi yang dipersoalkan; atau

☐ sebab-sebab lain seperti yang dibenarkan dibawah Akta Perlindungan Data Peribadi Malaysia:_____

_____

Nama Kakitangan: Tandatangan dan tarikh:

_____ _____

KOD TATA AMALAN PERLINDUNGAN DATA PERIBADI

UNTUK SEKTOR PENERBANGAN MALAYSIA

21 NOVEMBER 2017