A. RB Comments

No.	Section	Section Title	Comments
1.	3.1	**Definition of Personal Data**	Under the PDPO, "personal data" is defined to mean "*data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access*". Seeking clarification on point (b). The definition of personal data can either be *data, whether true or not, about an individual who can be identified (a) from that data;* ***OR*** *(b) from that data and other information to which the organisation has or is likely to have access*". If a personal data is data *and other information to which the organisation has or is likely to have access* but is not identifiable to an individual, would this still be considered as personal data as defined in the PDPO? Should it be "and" instead of "or"? Our current understanding of the definition of Personal Data is that Personal data only includes information relating to natural persons who: • can be identified or who are identifiable, directly from the information in question; or • who can be indirectly identified from that information in combination with other information.
2.	3.2	**Categories of Personal Data**	It is noted that the PDPO does not expressly recognise a distinction between sensitive and non-sensitive categories of personal data or define a category of "sensitive personal data". Our current policy dictates that sensitive data requires express consent whereas non-sensitive data may be processed by RB if RB has the lawful basis to do so without requiring express consent from the data subjects. Does this mean RB will be able to process sensitive data without requiring consent so long as RB has the lawful basis to do so?
3.	4.5	**The Accountability Obligations**	Under the Accountability Obligation in the PDPO, an organisation must appoint a person to be responsible for ensuring that it complies with the PDPO, typically referred to

			as a data protection officer ("**DPO**"); and develop and implement policies and practices that are necessary to meet its obligations under the PDPO, including a process to receive complaints. In addition, the organisation is required to communicate to its staff information about such policies and practices and make information available upon request to individuals about such policies and practices. <u>To what extent is the Brunei Data Office's role when it comes to the management of DPOs in Brunei?</u> RB is currently a certified organisation with the UK Information Commissioner's Office (ICO). In order to be certified by ICO, RB is required to pay an annual data protection fee of GBP2,900 and to submit all relevant policies for compliance purposes. <u>Is the Brunei Data Office considering setting up a DPO registry in Brunei?</u> We do believe that such certification will be beneficial for compliance purposes. Certification is a way for an organisation to demonstrate compliance with PDPO and enhance transparency. Certification can be utilized by customers as a means to quickly assess the level of data protection of particular product, process or service, which provides transparency both for customers and in business to business relationships.
4.	4.6.1	**The Consent Obligation**	The PDPO only dictates that an individual's consent is required before an organisation can collect, use or disclose such individual's personal data, unless otherwise required or authorised by law or an exception in the PDPO applies. The PDPO is silent on personal data of children. <u>What will be the PDPO's approach when it comes to personal data of children?</u> We believe that children need additional protection when an organization is collecting and processing their personal data because they may be less aware of the risks involved. To illustrate, RB current policy (as per GDPR) is drafted to follow the following general rules: • If an organisation rely on consent as the lawful basis for processing personal data, only children aged 13 or over are able provide their own consent. • For children aged 12 and below, an organisation need to get consent from whoever holds parental responsibility for

			them. The organisation must make reasonable efforts (using available technology) to verify that the person giving consent does, in fact, hold parental responsibility for the child. • If an organization wish to enter into a contract with a child, the organization must consider their competence to agree to the contract and understand the implications of the associated processing of their personal data. This means the child must be at the legal age of capacity to enter into the contract.
5.	4.6.4	**Deemed Consent**	Deemed Consent: There are circumstances where consent may be deemed under the PDPO, broadly: (a) if the individual, without giving express consent, voluntarily provides the personal data for that purpose; and it is reasonable that the individual would voluntarily provide the data; (b) if the collection, use or disclosure of the personal data is reasonably necessary for the conclusion of the contract between the individual and the organisation; and (c) if the organisation, after conducting a prescribed assessment for adverse effect on the individual, notify the individual of the new purpose and provide a reasonable period of time for them to opt out (provided that the individual does not opt out or otherwise withdraw their consent). As our current policy is drafted based on GDPR, GDPR dictates the following lawful basis for processing: a) **Consent:** the individual has given clear consent for organisation to process their personal data for a specific purpose. b) **Contract:** the processing is necessary for a contract organisation have with the individual, or because they have asked organisation to take specific steps before entering into a contract. c) **Legal obligation:** the processing is necessary for organisation to comply with the law (not including contractual obligations). d) **Vital interests:** the processing is necessary to protect someone's life.

			e) **Public task:** the processing is necessary for organisation to perform a task in the public interest or for organisation official functions, and the task or function has a clear basis in law. f) **Legitimate interests:** the processing is necessary for organisation legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if organisation are a public authority processing data to perform organisation official tasks.) <u>How would the PDPO consider deemed consent for circumstances for compliance with legal obligation, vital interests, public tasks or legitimate interests?</u> Other than lawful processing with consent or for fulfillment of contractual obligations with our customers, please note that RB may be required by law or upon request by governmental or regulatory authorities to submit personal data our RB passengers for various reasons e.g. compliance with immigration laws, assisting with criminal investigations, random security checks etc. Non-exhaustive list of regulatory or governmental authorities: Border Control/immigration/Custom Authorities, Anti-Corruption Bureau, Narcotics Control Bureau and Airport Police
6.	4.13	**The Transfer Limitation Obligation**	Under the Transfer Limitation Obligation, an organisation must not transfer personal data to a country or territory outside Brunei Darussalam except in accordance with requirements prescribed under the PDPO to ensure that the transferred personal data will be accorded a standard of protection that is comparable to that under the PDPO. In this regard, some jurisdictions (e.g. EU) impose stringent and prescriptive conditions in relation to transfer of personal data outside of its territories. In contrast, the PDPO places the onus on the organisation to ensure that appropriate measures are taken to protect personal data transferred out of Brunei through the imposition of contractual obligations or otherwise. <u>As the PDPO places onus on the organization to ensure appropriate measures are taken, is there minimum requirements place on the organization by the data office?</u>

			Would the Brunei Data Office prescribe certain level of standards for such measures?
7.	4.14.1	**The Data Breach Notification Obligation**	Under the PDPO, organisations are required to, as soon as practicable, but in any case, no later than 3 calendar days after making the assessment, notify the Responsible Authority of a data breach that: (a) results in, or is likely to result, in significant harm to the individuals to whom any personal data affected by a data breach relates; or (b) is or is likely to be, of a significant scale. Is failure to report be considered as a punishable office under the PDPO?
8.	5.1	**Data Subject Rights**	The PDPO will give individuals four main rights: 5.1.1 Right to withdraw consent; 5.1.2 Right to request access to personal data; 5.1.3 Right to request a correction of an error or omission in the personal data; and 5.1.4 Right to data portability. We duly note that Section 4.8 specifies the organisation's obligation to provide the individual with information on: (a) the purposes for the collection, use or disclosure of his personal data, on or before collecting the personal data; and (b) any other purpose for the use or disclosure of personal data that has not been notified to the individual, before such use or disclosure of personal data. Will the PDPO consider listing "the right to be informed" as one of the rights of data subjects? We understand that the notification obligation puts more weight on the organization to notify the data subjects. Nevertheless, we are of the view that data subjects must also be made aware of their right to be informed. Individuals should have the right to be informed about the collection and use of their personal data and in the way the PDPO is drafted, they may not be aware of such right as the PDPO only place an emphasis on the organisation's notification obligation. The right to be informed is a key transparency requirement under

			the GDPR. As such, right to be informed should form part of data subject rights under PDPO.
9.	8.1	**Do Not Call ("DNC") Regime**	The PDPO may provide for the establishment of a DNC regime. Individuals may request for their telephone numbers to be added to the DNC Registry if they do not wish to receive telemarketing messages via phone call, text message (i.e. SMS, MMS or any electronic communications sent using a telephone number, e.g. WhatsApp, Telegram) or fax. The DNC Registry will be administered by the Responsible Authority. Please confirm if the DNC registry is only limited to telemarketing messages via phone call, text message (i.e. SMS, MMS or any electronic communications sent using a telephone number, e.g. WhatsApp, Telegram) or fax? Are marketing emails excluded from the DNC obligation?

B. Conclusion

RB has conducted an extensive company-wide exercise when the EU General Data Protection Regulations was established in 2018. For purposes of planning, drafting and implementing policies, SOPs, privacy notices as such in order to comply with EU GDPR, RB relied on the UK Information Commissioner's Office (ICO), being the relevant state authority for RB, for guidance and all relevant information was provided by ICO via its website. We wish to highlight the following which were proven to be beneficial to RB during the implementation of EU GDPR:

- Guide to GDPR is provided in https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr).
- ICO also provide self-assessment toolkits where organisations may use the checklists to assess their compliance with data protection in order to find out what needs to be done within the organization. The self-assessment checklists is provided in https://ico.org.uk/for-organisations/sme-web-hub/checklists/data-protection-self-assessment/.

We believe that the Brunei Data Office should also put in place a guide to PDPO in a format similar to the ICO Guide to GDPR so as all relevant organisations will have access to PDPO provisions, guidance notes, templates and samples and this will also ensure a more controlled and standardised implementation of the PDPO nationwide. An example of self-assessment compliance survey is enclosed herewith in Annex A.

Importantly, the policy and implementation has to be a holistic one model approach with involvement of other government and non-government agencies. The success of the PDPO also lies in the practicality of implementing and documenting the data protection process throughout all organisations within Brunei and to take into consideration external parties.

Annex A

Survey on European Union (EU) General Data Protection Regulation (Regulation 2016/679 – GDPR)

Airline: _____

Awareness	
1. Is your airline aware of the EU GDPR coming into force on 25 May 2018?	
2. Is your airline aware if it is in scope?	
GDPR compliance strategy	
1. Who is in-charge of ensuring GDPR compliance within your airline?	
2. What other departments are involved?	
3. Briefly describe the reporting structure of the above	
4. Does your airline have a dedicated team looking at the GDPR compliance? If yes, how many persons are in the team?	

5. Does your airline engage external assistance to comply with the GDPR requirements? (e.g. legal counsel, management consultants, IT providers etc.?)	
Data Protection Officer (DPO)	
1. Is your airline planning to appoint a DPO?	
2. Where will the DPO located?	
3. Describe briefly the reporting structure of the DPO	
External partners	
1. Are your airline's external partners aware of the GDPR? (e.g. Airline partners, GDS, GSAs, GHAs, Travel Agencies, online partners, banks, hotels, car rentals, etc.)	

2. Have your airline engaged with external partners to ensure compliance with the GDPR?	