Group Personal Data Policy and Guidelines

September 2019

A. POLICY

1. Purpose

1.1 This document contains Swire Pacific's policy and general guidelines relating to Personal Data.

1.2 In this document:-

(a) "**Personal Data**" means any information (e.g. name, contact detail, passport number, biometric data, health data etc.) relating to an identified or identifiable natural person (e.g. customer, employee etc.);

(b) references to "**Swire Pacific**" are to Swire Pacific Limited and its subsidiaries (each a "**Swire Company**");

(c) references to "**Relevant Persons**" are to all employees of Swire Companies; and

(d) references to "**Division(s)**" are to the respective groups of Swire Companies under the following divisions: (i) Property, (ii) Aviation (for the avoidance of doubt, excludes Cathay Pacific), (iii) Beverages, (iv) Marine Services, and (v) Trading & Industrial.

1.3 Please refer to **Section J** of this document for other definitions.

2. Our Policy

2.1 It is the policy of Swire Pacific to comply with applicable legal requirements relating to the handling of Personal Data (including the collection, holding, processing, disclosure and use of Personal Data) (the "**Applicable Personal Data Laws**"). The privacy of others and the confidentiality of information received in the course of business must be respected.

2.2 Failure to comply with the Applicable Personal Data Laws may be an offence and may subject Swire Pacific and/or the Relevant Persons to fines and/or imprisonment. Swire Pacific may also suffer commercial, reputational or other disadvantages by failing to comply with the Applicable Personal Data Laws.

2.3 **Sections B to I** of this document set out the general guidelines on handling Personal Data. Divisions should comply with these general guidelines.

2.4 Divisions should carefully review their current operations and comply with any other relevant requirements under the Applicable Personal Data Laws.

B. DATA PROTECTION OFFICER

1. Appointment of Data Protection Officer

1.1 Each division should appoint a data protection officer ("**DPO**"). The DPO should be appointed on the basis of professional qualities or expert knowledge of Personal Data laws and practices, and be responsible for overseeing the division's compliance with the Applicable Personal Data Laws.

2. Responsibilities of Data Protection Officer

2.1 In particular, the DPO should be responsible for:-

(a) formulating detailed Personal Data governance policies, guidelines, standards, and procedures appropriate for his/her division ("**Division Guidelines**") to ensure compliance with the Applicable Personal Data Laws;

(b) coordinating with the business units within his/her division to implement the Division Guidelines;

(c) reviewing and approving PIAs (as defined in Section C1.1);

(d) put in place an incident response plan and procedures for his/her division. Such plan and procedures should cover data breach incidents and should provide guidance to senior management of the division on the proper handling, escalation and reporting of the data breach incidents;

(e) promoting staff awareness by conducting Personal Data trainings from time to time; and

(f) such other matters as may be required to be performed by a DPO under the Applicable Personal Data Laws.

C. COLLECTION OF PERSONAL DATA

1. Privacy Impact Assessment

1.1 **Before** collecting any Personal Data, divisions **should carry out** a **privacy impact assessment** ("**PIA**") to evaluate the proposed collection with a view to avoiding or minimising adverse impacts on privacy. Please refer to **Appendix I** for details on what a PIA should generally include.

1.2 The PIA should be reviewed and approved by the DPO before any Personal Data is collected.

2. Collection of Personal Data

General Principles

2.1 Divisions should only collect Personal Data if it is **necessary** for a **lawful purpose directly related** to their respective functions or activities. Collection of Personal Data **cannot be excessive**.

2.2 Personal Data should only be collected in a **lawful and fair** manner.

2.3 Personal Data may be classified into different categories (e.g. sensitive Personal Data and children's Personal Data etc.) under the Applicable Personal Data Laws. Divisions should comply with any additional legal requirements in relation to the handling of different categories of Personal Data imposed by the Applicable Personal Data Laws.

Personal Information Collection Statement

2.4 **On or before** collecting any Personal Data from a Data Subject, Swire Company **should provide or present** a **Personal Information Collection Statement** ("**PICS**") to the Data Subject. The PICS should be provided or displayed **in a clear and conspicuous manner**.

2.5 The purpose of the PICS is to provide the Data Subject with information relating to the collection and handling of his/her Personal Data collection. Such information should include:-

(a) the **purpose(s)** of collecting the Personal Data (i.e. what the Personal Data will be used for);

(b) the **classes of persons** which the division may transfer Personal Data to (for non-Direct Marketing purpose);

(c) whether it is **obligatory or voluntary** for the Data Subject to provide his/her Personal Data. If it is obligatory, include the consequences of failing to provide;

(d) if the division intends to use the Personal Data collected for Direct Marketing purposes:-

(i) inform the Data Subject regarding such intention;
(ii) inform the Data Subject that the division may not use his/her data unless it has received his/her consent;
(iii) provide **specific** information about the kinds of Personal Data (e.g. name and email address) ("**Kinds of Personal Data**") to be used for Direct Marketing purpose;
(iv) provide **specific** information about the classes of Marketing Subjects (e.g. beauty products offered by ABC Company) ("**Classes of Marketing Subjects**") in relation to which the Personal Data is to be used;
(v) specify the response channel (e.g. email or postal address) through which the Data Subject may (at no cost) communicate his/her consent.

(e) if the relevant Swire Company intends to transfer or provide the Personal Data collected to third parties (including another Swire Company) for their use in Direct Marketing:-

(i) inform the Data Subject regarding such intention;
(ii) inform the Data Subject that the collecting Swire Company may not transfer or provide such data unless it has received the Data Subject's written consent;
(iii) (if applicable) inform the Data Subject that his/her Personal Data is to be transferred or provided **for gain** (i.e. in return for money or other property);
(iv) provide **specific** information about (A) the Kinds of Personal Data to be transferred or provided, (B) the classes of persons to which the Personal Data is to be transferred or provided (e.g. marketing or research service providers) ("**Classes of Persons**"), and (C) the Classes of Marketing Subjects in relation to which the data is to be used;

(f) the **rights** of the Data Subject (e.g. rights to data access and correction) under the Applicable Personal Data Laws;

(g) the **name (or job title) and contact details** of the person responsible (e.g. DPO) for handling data enquiries or requests; and

(h) any other information as may be required to be provided to Data Subjects under the Applicable Personal Data Laws. For example, regarding the Classes of Persons, certain Applicable Personal Data Laws require the full entity name of the transferee (e.g. ABC Company Limited) to be specified in the PICS.

2.6 Divisions should consider whether any general, specific and/or written consent(s) from a Data Subject to the PICS and/or any intended use or transfer of his/her Personal Data is required according to the Applicable Personal Data Laws.

Collecting Personal Data of Data Subjects from Third Parties

2.7 If Personal Data of Data Subjects will be collected from a third party (instead of directly from the Data Subjects), divisions should consider if written confirmation from the third party (regarding e.g. the third party's compliance with the Applicable Personal Data Laws in relation to the transfer and use of the Personal Data) is required to be obtained under the Applicable Personal Data Laws.

3. Data Privacy Policy

3.1 Divisions should have in place a public policy or statement ("**Data Privacy Policy**") containing the following information:-

(a) its policies and practices in relation to Personal Data;

(b) the Kinds of Personal Data held by it;

(c) the main purposes for which Personal Data held by it is used; and

(d) any other information which is required by the Applicable Personal Data Laws to be made available to the public.

3.2 To ensure a person can ascertain a division's Data Privacy Policy in relation to Personal Data, the division should display its Data Privacy Policy in a clear and conspicuous manner on all its websites.

3.3 If it is considered legal and appropriate to do so, divisions may combine the PICS and its Data Privacy Policy into one document.

4. Cookies or Other Online Behavioural Tracking Technologies

4.1 Online behavioural tracking includes recording users' identity, dealings and/or behaviour on websites through the use of cookies or other techniques.

4.2 If divisions engage in online behavioural tracking, they should comply with the relevant requirements under the Applicable Personal Data Laws. This may include publication of a cookies policy on websites where online behavioural tracking activities are conducted.

D. USE AND TRANSFER OF PERSONAL DATA

1. Use of Personal Data

1.1 Divisions should use, disclose, process or transfer Personal Data **only for the purpose(s) of which the Data Subject was informed** (and if applicable, to which the Data Subject has consented).

1.2 If Personal Data will be used, disclosed or transferred for any **other** purpose (i.e. a 'new purpose'), the relevant Swire Company **must first obtain consent** from the Data Subject.

1.3 Requirements on the use and transfer of certain categories of Personal Data (e.g. sensitive Personal Data and children's Personal Data) may be more stringent under different Applicable Personal Data Laws, divisions should carefully review the requirements under the Applicable Personal Data Laws and comply with such requirements accordingly.

2. Use of Publicly Available Personal Data

2.1 When a third party (e.g. a professional body) make certain Personal Data publicly available (e.g. telephone directories) and has specified the purposes for which such data may be used (e.g. to make business contact), the relevant Swire Company may use such Personal Data only for such specified purposes. If the purposes are not stated, the relevant Swire Company should consider the reasonable privacy expectation of the individuals (i.e. whether a reasonable person would find the re-use of the data unexpected or inappropriate).

2.2 Divisions must not use Personal Data collected from the public domain for Direct Marketing purposes.

3. Transferring Personal Data to Third Parties

3.1 Before transferring any Personal Data to a third party (including a Swire Company), the transferring Swire Company should inform the third party of the purposes of providing the Personal Data to it. The purposes should be any of those purposes set out in the PICS which the transferring Swire Company provided to the relevant Data Subjects. This is to avoid the third party misusing the data.

3.2 Under certain Applicable Personal Data Laws, there may be a requirement to enter into a written agreement with the third party imposing data protection obligations on the third party before any Personal Data can be transferred.

3.3 Divisions are reminded to comply with the other applicable requirements set out in this document relating to the transfer of Personal Data to third parties (e.g. the data processing requirements under **Section E** of this document).

4. Obtaining Personal Data from Third Parties

4.1 Before obtaining any Personal Data from a third party (including a Swire Company), the obtaining Swire Company should ask the third party to specify the purposes which the Personal Data may be used for. Divisions are reminded to review whether a written agreement relating to such transfer is required to be entered into with the third party under the Applicable Personal Data Laws.

4.2 If the relevant Swire Company intends to use the Personal Data received from the third party for Direct Marketing purposes, it should first **obtain written confirmation from the third party** regarding the following:-

(a) the third party has complied with the Applicable Personal Data Laws in relation to the transfer or disclosure of Personal Data;

(b) the third party has **given written notice** to the Data Subject and **obtained his/her written consent** to the transfer or disclosure of Personal Data;

(c) the use of the Personal Data by the division is consistent with the consent obtained by the third party from the Data Subject; and

(d) any other confirmation which is required by the Applicable Personal Data Laws to be obtained from the third party before the division can use the Personal Data for Direct Marketing purposes.

5. Cross-border Transfer of Personal Data

5.1 Laws governing cross-border transfer of Personal Data vary across jurisdictions. For instance, certain Applicable Personal Data Laws require certification and adherence to approved codes of conduct before any Personal Data can be transferred abroad. Divisions should review the Applicable Personal Data Laws to ensure compliance.

E. DATA PROCESSING

1. Pre-Contractual Due Diligence

1.1 Before engaging a Data Processor, divisions should conduct due diligence on the Data Processor.

1.2 Divisions should consider if the Data Processor is fit for the intended engagement. The Data Processor should have the capacity, experience, and sufficient technical and security measures in place to safeguard the Personal Data.

2. Contractual Arrangement

2.1 Before transferring any Personal Data to a Data Processor, the relevant Swire Company must ensure that a written agreement is entered into with the Data Processor.

2.2 The written agreement should impose the following data protection obligations on the Data Processor:-

(a) timely return, destroy or delete the Personal Data when it is no longer required for data processing. If appropriate and practicable, specify a reasonable period within which the Data Processor should return, destroy or delete the Personal Data;

(b) adopt appropriate and necessary security measures to protect the Personal Data from unauthorised or accidental access, processing, erasure, loss or use;

(c) prohibit the use (or disclosure) of Personal Data for any purpose other than in pursuance of the data processing;

(d) prohibit absolutely (or allow with restrictions) the sub-contracting of the data processing services. If sub-contracting is allowed, the Data Processor's agreement should impose the same obligations on the sub-contractor. If the sub-contractor fails to fulfill its obligations, the Data Processor shall remain fully liable;

(e) immediately report to the division any sign of abnormalities or security breaches;

(f) take measures to ensure that its relevant staff will carry out the security measures and comply with the above obligations (e.g. the Data Processor should have Personal Data protection policies in place and provide adequate training to its relevant staff);

(g) allow the division to audit and inspect how the Data Processor handles and stores Personal Data;

(h) comply with all relevant requirements under the Applicable Personal Data Laws; and

(i) be responsible for its violation of the contract, and specify the consequences of violation.

F. DATA ACCURACY, RETENTION AND ERASURE

1. Data Accuracy

1.1 Divisions should take all practicable steps to ensure that Personal Data held is **accurate** having regard to the **purposes for which the data is to be used** (the "**Purposes**").

2. Data Retention

2.1 Divisions should take all practicable steps to ensure that Personal Data is **not kept longer than is necessary** to fulfil the Purposes.

2.2 Divisions should put in place retention policies that specify the retention period of the Personal Data they hold.

3. Data Erasure

3.1 Divisions should take all practicable steps to erase the Personal Data they hold (a) when such data is **no longer required** for the Purposes; or (b) upon a Data Subject's request to the extent the Division considers appropriate or is legally required to do so.

3.2 Personal Data must be destroyed or erased **properly and securely**. When disposing of storage holding Personal Data, practicable steps should be taken to ensure that the data is erased and cannot be retrieved.

3.3 Divisions should put in place procedures (including the means to identify and gather all copies) for proper erasure of Personal Data, and maintain erasure records.

G. SECURITY OF PERSONAL DATA

1. General Principle

1.1 Divisions should take all practicable steps to ensure that Personal Data are protected against **unauthorised access, alteration, loss or processing** having regard to:-

(a) the kind of data, and the harm that could result;

(b) the location where data is stored;

(c) any security measures for equipment in which data is stored;

(d) any measures to ensure the suitability of staff having access to the data; and

(e) any measures to ensure the secure transmission of the data.

2. Access Control

2.1 Personal Data must be accessed only on a **"need-to-know/use" basis**. Divisions should (a) determine the access rights of its staff; and (b) implement proper authorisation and verification procedures for access.

2.2 Divisions are responsible for reminding their staff about Personal Data privacy and security issues, and must be satisfied that staff who are given access to Personal Data are sufficiently briefed on these issues.

3. Storage / Security Measures

3.1 Personal Data (in whatever form) must be **securely stored** at all times. Unnecessary copies of Personal Data should not be created or kept.

3.2 Divisions should adopt appropriate security measures to protect unauthorised access or alteration to Personal Data.

H. DATA SUBJECTS REQUESTS

1. Data Access Request

1.1 A Data Subject is entitled to ascertain whether a Swire Company holds his/her Personal Data and, if so, obtain a copy of such data.

1.2 Divisions should comply with a Data Subject's data access request according to and within the prescribed period under the Applicable Personal Data Laws.

2. Data Correction Request

2.2 A Data Subject may request for a correction of his/her Personal Data.

2.3 If the old Personal Data is inaccurate, (a) necessary correction should be made based on the Data Subject's request; and (b) a copy of the corrected data should be provided to the Data Subject within the prescribed period under Applicable Personal Data Laws.

3. Opt-Out Request

3.1 If a Data Subject requests a Swire Company to cease using his/her Personal Data (or cease providing his/her Personal Data to others for their use) in Direct Marketing ("**Opted-Out**"), the division should comply with the request accordingly.

3.2 Divisions should maintain lists of all Data Subjects who have Opted-Out, and such lists should be updated regularly.

4. Other Requests

4.1 Data Subjects may be entitled to other rights (e.g. data erasure/masking requests, a right to be forgotten, a right to restriction of processing and/or a right to data portability) under the Applicable Personal Data Laws. Divisions should review their operations and comply with the relevant requests according to the Applicable Personal Data Laws.

I. DATA BREACH HANDLING

1. Data Breach Definition

1.1 Data breach means a breach of security of the Personal Data held by a division (or its Data Processor or joint data owner).

1.2 Examples of data breach are:-

- Loss of storage devices that contain Personal Data
- Accidental or unauthorised transmission or disclosure of Personal Data
- Database containing Personal Data being hacked

2. Incident Response Plan

2.1 Divisions should establish an incident response plan which sets out the following in relation to handling a data breach incident:-

(a) establishment and composition of an incident response team ("**IRT**");

(b) roles and responsibilities of each IRT member;

(c) escalation procedure, communications and response actions (including damage control); and

(d) investigation and post-incident analysis.

2.2 Divisions should consider whether data breach notification(s) to Data Subjects and/or relevant regulatory authorities are required or appropriate, having regard to the Applicable Personal Data Laws.

J. DEFINITIONS

The definitions of the following terms, although commonly used, may vary between different jurisdictions. The following defined terms are included as a reference, and divisions should review their corresponding definitions under the Applicable Personal Data Laws.

"**Data Processor**"	means a person who:- - processes Personal Data on behalf of another person; and - does not process the data for any of its own purposes. *E.g. Service companies engaged to input Personal Data to computer systems or shred confidential documents which contain Personal Data, on behalf of another person.*
"**Data Subject**"	means the individual who is the subject of the Personal Data (e.g. customer, employee etc.).
"**Direct Marketing**"	means:- - the offering (or advertising of the availability) of goods, facilities or services to a natural person, or - the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes from a natural person.
"**Marketing Subject**"	in relation to Direct Marketing, means:- - any goods, facility or service offered, or the availability of which is advertised, or - any purpose for which donations or contributions are solicited.
"**process**" or "**processing**"	means any operation which is performed on Personal Data (whether or not by automated means). *E.g. collection, recording, analysing, profiling, amending, augmenting, deleting, structuring, storage, retrieval, rearranging, use, disclosure, dissemination, combining, restriction, erasure or disposal of Personal Data.*

Appendix I
Privacy Impact Assessment

A privacy impact assessment ("**PIA**") should at least involve the following:-

1. Data Processing Cycle Analysis

1.1 Examine the **purpose** and the **rationale** behind the project to decide **whether it is necessary** to collect such **kind**, **amount** and **extent** of Personal Data.

1.2 To the extent practicable, adopt the less privacy-intrusive alternatives.

1.3 Ensure the guidelines set out in this document and the Division Guidelines can be complied with.

2. Privacy Risks Analysis

2.1 Analyse the relevant privacy risks. In doing so, one should take into account the following:-

(a) the functions and activities of the Swire Companies within the division;

(b) the nature and the Personal Data involved;

(c) the number of individuals affected;

(d) the gravity of harm to the Data Subjects if their Personal Data is improperly handled;

(e) whether a Data Processor is (or will be) appointed to carry out data processing; and

(f) the privacy standards and rules prescribed under the Applicable Personal Data Laws and any applicable codes of practices, guidelines and regulations that the division shall observe, etc.

2.2 In general, the level of Personal Data protection measures which the division is required to take should be proportionate to the privacy intrusiveness of the project.

3. Avoiding or Mitigating Privacy Risks

3.1 To the extent practicable, **avoid** the privacy risks or **adopt appropriate mitigating measures** to protect the Personal Data from unauthorised access, processing, erasure, loss or use.

4. Clear Documentation

4.1 The PIA should be clearly documented. This should include the findings, recommendations and the privacy risk mitigating measures that are proposed to be adopted for the project.

4.2 The PIA report may include the following:-

(a) a description of the project;

(b) the data processing cycle analysis highlighting the circumstances in which the Personal Data is collected and processed (whether by the Data User or by its data processing agent);

(c) identification of the relevant privacy risks; and

(d) the ways and means used to properly address or mitigate these risks and to explain (in sufficient detail) how any less privacy-intrusive alternatives have been considered and where appropriate, why they have not been adopted.