Personal Data Incident Notification Policy (Philippines)

1 SCOPE

1.1 This personal data incident notification policy for the Philippines (the "**Policy**") applies to Vouvray Acquisition Limited and its subsidiaries and/or affiliates (together "**V.Group**"). All Colleagues are required to follow this procedure in the event of a Personal Data Breach.

1.2 This Policy:

(a) forms part of V.Group's Data Protection Policy (Philippines) (www.vgrouplimited.com/Data-Protection-Overview-Philippines.aspx); and

(b) may be amended by V.Group at any time, consistent with the requirements of applicable laws and regulations. Any revisions will take effect from the date on which the amended Policy is published, as indicated in the version number set out herein.

2 DEFINITIONS

2.1 "**Colleague**" is as defined in the Data Protection Policy (Philippines);

"**Data Subject**" is as defined in the Data Protection Policy (Philippines);

"**Data Protection Committee**" means the data protection committee of V.Group including the Global DPO; it may be contacted at data.protection@vgrouplimited.com;

"**Global DPO**" means the data protection officer for V.Group globally and for GDPR purposes as set out in Schedule 1;

"**Group IS**" means the information systems department of V.Group;

"**Group Legal**" means the legal department of V.Group; it may be contacted via legal@vgrouplimited.com;

"**Internal Breach Register**" means the internal breach register which details any Personal Data Breaches;

"**Personal Data**" is as defined in the Data Protection Policy;

"**Philippines DPO**" means the data protection officer for V.Group in the Philippines as set out in Schedule 1;

"**pseudonymised data**" means the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not

attributed to an identified or identifiable natural person and "**pseudonymised**" and "**pseudonymisation**" shall be construed accordingly.

"**Sensitive Personal Data**" is as defined in the Data Protection Policy;

"**Supervisory Authority**" means an independent public authority responsible for monitoring the application of the applicable Philippines data privacy laws including the DPA.

2.2 Words denoting the singular shall include the plural and vice versa.

2.3 Unless otherwise stated, all defined terms have the same meaning as defined in the Data Protection Policy (Philippines).

3 WHAT IS A PERSONAL DATA BREACH?

3.1 A "**Personal Data Breach**" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

3.2 Examples of Personal Data Breaches are:

(a) "Confidentiality breach" – an unauthorised or accidental disclosure of or access to Personal Data;

(b) "Availability breach" – an unauthorised or accidental loss of access to or destruction of Personal Data;

(c) "Integrity breach" – an unauthorised or accidental alteration of Personal Data.

4 PERSONAL DATA BREACH AND PERSONAL DATA INCIDENT

4.1 Section 3.1 defines what a Personal Data Breach is.

4.2 A "**Personal Data Incident**" is a possible, potential or suspected Personal Data Breach. It is essential that you understand the distinction between a Personal Data Breach and a Personal Data Incident, i.e. a Personal Data Incident is not necessarily a Personal Data Breach.

4.3 **If there has been a Personal Data Incident, any Colleagues involved should refer to the Personal Data Incident as an "incident" and should not refer to it as a "breach" (particularly when communicating in writing/by email).**

4.4 It is for the Global DPO to determine whether a Personal Data Incident constitutes a Personal Data Breach.

5 PROCEDURE – ASSESSING A PERSONAL DATA INCIDENT

5.1 Notify Philippines DPO and Global DPO

(a) V.Group may be required to report Personal Data Breaches to the supervisory body no later than 72 hours after becoming aware of it. Due to this requirement, **you must report all Personal Data Incidents (i.e. all *possible, potential or suspected* Personal Data Breaches) to the Philippines DPO and Global DPO immediately and in any event within 24 hours of becoming aware of the Personal Data Incident**.

(b) If in doubt as to whether a Personal Data Incident or Personal Data Breach has occurred, you are required to err on the side of caution and report it.

(c) The Personal Data Incident notification needs to be made by email:

(i) to the Philippines DPO at the appropriate email address:

(A) dpo.vso@vships.com

(B) dpo.ksi@vships.com

(C) dpo.nsmsc@vships.com

(D) dpo.pomi@vships.com

(E) dpo.ohtc@vships.com

(ii) with a copy to the Data Protection Committee (at data.protection@vgrouplimited.com);

(iii) marked as "High Importance"; and

(iv) with the following in the Subject line: "Private, confidential and legally privileged – Personal Data Incident".

5.2 The Philippines DPO will confirm receipt of this information by email.

5.3 Each Personal Data Incident must have a risk assessment performed to determine the extent and risk to the Personal Data. The risk assessment is based on facts and determines whether the Personal Data was used or disclosed in a way not permitted under V.Group's policies. The risk assessment includes an evaluation of whether the incident compromises an individual's Personal Data.

5.4 The following participate in a risk assessment: Philippines DPO, Global DPO, Group IS and Group Legal.

5.5 For the risk assessment the following steps will be carried out:

(a) Data list:

A detailed list and description of the data involved in the Personal Data Incident needs to be prepared. The list must include all the Personal Data which is potentially at risk as a result of the incident.

(b) Security controls applied to the data:

Any security controls applied to the data may limit unauthorised exposure. This may include encryption, pseudonymisation, access controls or any other controls. The security controls applied to the data should be documented.

(c) Determination of risk to the individual:

The level of risk to the individual will determine whether the Personal Data Incident is to be notified to the Supervisory Authority and/or the affected Data Subject. Determining the risk requires an evaluation of:

(i) the facts surrounding the Personal Data Incident;

(ii) an examination of the type of Personal Data;

(iii) the potential harm to the individual; and

(iv) security controls applied.

(d) Forensic investigation:

Group IS is responsible for conducting computer forensics in support of investigations. Group IS must be engaged at the earliest opportunity when suspicious computer activity or security incidents occur to ensure information is properly gathered and handled during response efforts. No information (or structure of information) should be deleted, moved or changed in any way.

(e) Legal analysis:

The Philippines DPO and Global DPO will analyse the data identified under the 'data list', including the security controls applied and any risk to an individual, to consider whether the Personal Data Incident constitutes a Personal Data Breach.

5.6 The following factors (along with any other relevant considerations) will be considered to determine if Personal Data has been compromised (you need to ensure that this information is recorded and provided promptly in writing to the Philippines DPO):

(a) the nature of the Personal Data Incident including where possible, the categories and approximate number of individuals concerned, and the categories and approximate number of data records concerned;

(b) the nature and extent of the Personal Data involved, including where Personal Data was pseudonymised data, types of identifiers and the likelihood of re-identification;

(c) the identity of the unauthorised person who triggered the Personal Data Incident and, where applicable, or to whom it was disclosed;

(d) whether the Personal Data was actually acquired (including whether any security controls were applied to prevent access);

(e) the likely consequences of the Personal Data Incident; and

(f) the measures that could be taken to address the Personal Data Incident, including where appropriate, to mitigate any adverse effects.

5.7 If Personal Data is pseudonymised in accordance with applicable laws or guidance, it still qualifies as Personal Data and any inadvertent or unauthorised use or disclosure of such information will be considered a Personal Data Breach.

5.8 If Personal Data is anonymised in accordance with applicable laws and guidance, it is not Personal Data and any inadvertent or unauthorised use or disclosure of such information will not be considered a Personal Data Breach. Consult the Philippines DPO and Global DPO first to confirm if the data is truly anonymised.

5.9 It is important that systems and/or operations are restored as soon as possible, ensuring that this can be done without creating any further security issues or putting V.Group at risk of additional incidents or unintentionally discarding or destroying evidence.

5.10 Before any restoration of systems and/or data, the system should be tested to ensure it is no longer vulnerable or to prevent or minimise any potential future security risks.

6 PROCEDURE – BREACH NOTIFICATION TO SUPERVISORY AUTHORITY

6.1 If it is determined that the Personal Data Incident constitutes a Personal Data Breach, V.Group will assess in respect of the Personal Data Breach whether:

(a) it involves Sensitive Personal Data or other Personal Data that may be used to enable identity fraud;

(b) there is reason to believe that the Personal Data have been acquired by an unauthorised person; and

(c) the unauthorised acquisition is likely to result in a risk to the rights and freedoms of the Data Subjects affected by the Personal Data Breach, by conducting a Data Protection Impact Assessment,

such a risk if unaddressed is likely to have a significant detrimental effect on individuals – for example, resulting in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

6.2 If (a), (b), and (c) above are present, V.Group must report the Personal Data Breach to the Supervisory Authority without undue delay, and not later than 72 hours of becoming aware of the breach.

6.3 If it is not possible to provide all of the necessary information at the same time, V.Group will provide the information in phases without undue further delay. For the avoidance of doubt, even if all of the necessary information is not available, the Supervisory Authority must be contacted within the 72 hour deadline, be provided with the information that is available and reasons why the remaining information is not available – V.Group must submit a follow up report within five (5) days from knowledge, unless allowed a longer period by the Supervisory Authority.

6.4 The following information needs to be provided to the Supervisory Authority (you must ensure that this information is documented, so that it is available when required):

(a) a description of the nature of the Personal Data Breach;

(b) the date the Personal Data Breach occurred;

(c) the date the Personal Data Breach was discovered and any reasons why the breach was not notified within 72 hours (if applicable);

(d) the categories of Data Subjects affected;

(e) whether the Personal Data Breach involved pseudonymised data or anonymised data;

(f) approximate number of Data Subjects affected;

(g) the categories of Personal Data records affected;

(h) approximate number of Personal Data records affected;

(i) name and contact details of the Philippines DPO;

(j) the likely consequences of the breach; and

(k) any measures taken or proposed to be taken to address the Personal Data Breach, including where appropriate, to mitigate any adverse effects.

6.5 The Philippines DPO will notify the Supervisory Authority.

6.6 In the event the Supervisory Authority assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register.

6.7 The breach notification is made to the Supervisory Authority by email.

7 PROCEDURE – BREACH NOTIFICATION TO DATA SUBJECT

7.1 If the Personal Data Breach is likely to result in high risk to the rights and freedoms of the Data Subject, V.Group must notify the Data Subjects affected without undue delay, and not later than 72 hours of becoming aware of the breach, unless there is a reason to postpone or omit notification, subject to approval of the Supervisory Authority.

7.2 The notification to the Data Subject should describe the breach in clear and plain language and contain at least the following information:

(a) a description of the nature of the Personal Data Breach;

(b) the categories of Personal Data records affected;

(c) name and contact details of Philippines DPO;

(d) likely consequences of the Personal Data Breach;

(e) measures taken or proposed to be taken to address the Personal Data Breach, including where appropriate, to mitigate any adverse effects; and

(f) instructions on how the Data Subject will get further information and recommendation on how to minimize the risks resulting from the Personal Data Breach

7.3 Such notification to the Data Subject referred to is not required if exempted by the Supervisory Authority, after considering the following factors:

(a) V.Group has implemented appropriate technical and organisational protection measures, and those measures were applied to the Personal Data affected by the Personal Data Breach, in particular those that render the Personal Data unintelligible to any person who is not authorised to access it;

(b) V.Group has taken subsequent measures which ensure that the high risk to the rights and freedoms of Data Subjects referred are no longer likely to materialise; or

(c) the age or legal capacity of affected Data Subjects provided, that in the case of minors or other individuals without legal capacity, notification may be done through their legal representatives.

7.4 Consult the Philippines DPO and Global DPO first to confirm if any of the exceptions set out in Section 7.3 above apply.

8 INTERNAL REGISTER

V.Group must keep an Internal Breach Register documenting any Personal Data Breaches which include:

(a) the facts relating to the Personal Data Breach, its root cause and circumstances regarding its discovery;

(b) the effects of the Personal Data Breach;

(c) Actions and decisions of the Data Protection Committee;

(d) Outcome and difficulties encountered; and

(e) the remedial action taken.

9 DOCUMENT CONTROL

9.1 The Global DPO is the owner of this Policy and is responsible for ensuring that this procedure is reviewed in line with the relevant review requirements.

9.2 A current version of this Policy is available at www.vgrouplimited.com/Data-Protection-Overview-Philippines.aspx

9.3 This Policy was approved as stated in this Section and is issued on a version-controlled basis.

Version	Date of Issue	Approved by	Position	Company
1	18.04.2018	Allan Christensen	Head	V.Ships Services Oceana Inc.
		Kathryn Aguirre	Head	Kestrel Shipping, Incorporated
		Kathryn Aguirre	Head	North Sea Marine Services Corporation
		Elmer Pulumbarit	Head	Pacific Ocean Manning, Incorporated
		Arnold Guia	Head	Oceanic Hospitality Training Centre Corporation

Schedule 1

V.Group DPOs

DPO	Name	Email	Address	Telephone no.
Philippines DPO	Gerald Ambrosio	gerald.ambrosio@vships.com	9F Aseana Two Bldg., Bradco Ave., Aseana City, Paranaque City, Philippines 1702	+632 8589988
Global DPO	Beaummont Tang	dpo@vgrouplimited.com	V.Group, 1st Floor, 63 Queen Victoria Street, London, EC4N 4UA, UK	+44 207 3328510