DATA PRIVACY PROTECTION

VANPAC GROUPASIA – SINGAPORE

Vanpac GroupAsia collects data from a variety of sources for use in the services we provide to our customers. Bona fide privacy principles are essential to the proper protection and management of this data and the personally identifiable information ("PII") contained within this data. We believe and have adopted the Generally Accepted Privacy Principles of Notice/Awareness, Choice, Consent, Access and Security. Our Consumer Privacy Principles are outlined below:

MANAGEMENT

The Management of VPGA and our Consumer Privacy Principles include the definition, documentation, and communication related to the accountability of our privacy policies and procedures. In this regard, we support consumer education, developing industry standards and best practices, responsible and effective federal regulation of the industry, and legislation governing the practices of all data collectors. We also support industry oversight and active engagement with the privacy community and believe that strong privacy and information security protections are vital for an effective and trusted service industry.

Overview of data processing activities

Purposes of processing	Categories of individuals	Categories of personal data	Where it came from	Who it is shared with
Staff administration	Employees	Contact details	Employee	Relevant Parties
		Financial details		Accounts Department
	Emergency contacts	Contact details		Relevant Parties
Customer orders	Customers	Contact details	Customer	Relevant Parties
		Financial details		Relevant Department
		Personal Documents (Passport/Visa)		Permit Team
	Suppliers	Contact details	Supplier	Purchasing Department
		Financial details		Accounts Department
		Location		Relevant Parties
Marketing	Customers	Contact details	Customer	Marketing Department
	Clients	Contact details	Client	

NOTICE/AWARENESS

We are committed to the Privacy Principles of Notice and Awareness through documented policies and procedures, communication with our business partners, suppliers, clients, vendors, and providing information on our best practices to consumers through our Privacy Policies. Further, we believe in consumer awareness and transparency and provide via our staff.

CHOICE AND CONSENT

We respect consumer choice and allow consumers to Opt-Out of our services provided by us. Our Opt-Out

provisions are specified in the associated privacy policies located on our web site.

DATA COLLECTION, QUALITY, USE, RETENTION, AND DISPOSAL

When we collect information and data from our clients we maintain quality controls to ensure information is as accurate as possible. All information we collect are only necessary as per the work we conduct, namely in the customs dealing with import and export. We collect and use the information we collect in strict adherence to our data privacy agreements. We control and secure the use of information through technology and operational regulation in the office. All information are secured on our network. We limit the dissemination of VPGA through product controls. Data is retained and disposed in accordance with our retention policies, and will be 100% deleted once the requirements for retention are over.

We monitor and audit our business partners to ensure compliance with our contracted and legal requirements. To prevent any leaks and hacks, all staff are told to sign off and agree to not transfer any personal data outside of the office. IT department has also secured the network with industrial grade Anti Spy ware and Virus which prevents hacking against our data.

DATA ACCESS

Access is limited to the client and the move coordinator and their superiors only. No data should be shared unnecessarily and only accessed on a need-to-know basis.

DISCLOSURE TO THIRD PARTIES

We limit the distribution of VPGA in accordance with its level of sensitivity, its legal restriction on use, and in accordance with Singapore's PDPC guidelines.

SECURITY FOR PRIVACY

Data security is of utmost importance. We strive to protect VPGA from unauthorized access and inappropriate use and to prevent the inappropriate dissemination of VPGA through an effective, industry standard physical and logical security program. We have established and maintain strict guidelines and contracts for initializing, implementing, maintaining and improving security. In the event of an unintended breach, we maintain our commitment to respond to address the breach and any consumer notification requirements.

HOW TO HANDLE A DATA BREACH

1) Stop the breach
   - Isolate any system(s) access by the attacker so you can prevent the breach from spreading.
   - Disconnecting breached accounts/shutting down affected departments.
2) Assess the damage
   - Investigate how sensitive is the breached data
   - What type of data is affected
   - Does the data contain high-risk information
3) Notify those affected
   - Cite the date of the breach
   - Cite what was compromised and what the recipient can do to prevent further damage
4) Conduct a security audit
5) Update recovery plan to prepare for future attacks

QUALITY

We ensure the accuracy of any personal data we create.
We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data.
We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary.

MONITORING AND ENFORCEMENT

We maintain management oversight to ensure compliance with our DataPrivacy Principles. Additionally, we

also obtain independent assessments from qualified third-party entities when necessary to ensure that we maintain the appropriate administrative, technical, and physical safeguards necessary to protect VPGA and to solidify and continue to develop our Consumer Privacy

DEFINITIONS

Personal information: (sometimes referred to as personally identifiable information) information that concerns, or can be related to, an identifiable individual.

Individuals, for this purpose, include prospective, current, and former customers, employees, and others with whom the entity has a relationship. Most information collected by an organization about an individual is likely to be considered personal information if it can be attributed to an identified individual. Some examples of personal information are as follows:

- Name
- Home or e-mail address
- Date of Birth
- Identification number (for example, a Social Security or Social Insurance Number)
- Physical characteristics

Sensitive information: Some personal information is considered sensitive. Some laws and regulations define the following to be sensitive personal information:

- Information on medical or health conditions
- Financial information
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sexual preferences
- Information related to offenses or criminal convictions

Non-personal information:

Information about or related to people that cannot be associated with specific individuals. This includes statistical or summarized personal information for which the identity of the individual is unknown or linkage to the individual has been removed. In such cases, the individual's identity cannot be determined from the information that remains because the information is de-identified or anonymized. Non-personal information ordinarily is not subject to privacy protection because it cannot be linked to an individual. However, some organizations may still have obligations over non-personal information due to other regulations and agreements

PRIVACY OR CONFIDENTIALITY?

Unlike personal information, which is often defined by law or regulation, no single definition of confidential information exists that is widely recognized. In the course of communicating and transacting business, partners often exchange information or data that one or the other party requires be maintained on a "need to know" basis. Examples of the kinds of information that may be subject to a confidentiality requirement include the following:

- Transaction details
- Engineering drawings
- Business plans
- Banking information about businesses
- Inventory availability
- Bid or ask prices
- Price lists
- Legal documents
- Revenue by client and industry

Also, unlike personal information, rights of access to confidential information to ensure its accuracy and completeness are not clearly defined. As a result, interpretations of what is considered to be confidential information can vary significantly from organisation to organisation and, in most cases, are driven by contractual arrangements.

Explicit consent: "Explicit" in the data protection world generally means "specific". In other words the consent must specify the particular types of data, the specific purposes for which they may be used and/or the countries to which they may be disclosed.

Implicit consent: "Implicit" refers to "not specific" It is consent which is not expressly granted by a person or company, but rather inferred from a person or company's actions and the facts and circumstances of a particular situation.

Supply Chain: A Supply Chain is a system of organisations, companies, people, activities, information, and resources involved in moving a product or service from supplier to customer.

Supply Chain Management: The network created amongst different companies producing, handling and/or distributing a specific product or service. Specifically, the supply chain encompasses the steps it takes to get a good or service from the supplier to the customer. Supply chain management is a crucial process for many companies, and many companies strive to have the most optimized supply chain because it usually translates to being able to deliver a higher overall quality performance resulting in lower costs for the company.