PERSONAL DATA PROTECTION POLICY

WPG SOUTH ASIA

GROUP OF COMPANIES

8 MAY 2020

CONTENTS

1.0 Objective of the Policy

This Personal Data Protection Policy (the "Policy") is issued pursuant to the introduction of the new Personal Data Protection Act 2012 ("PDPA") which comes into full force on 2 July 2014 in the Republic of Singapore.

The objective of this Policy is to provide a guideline on the application of the PDPA in the collection, using, managing, storing and the disclosure of personal data in compliance with the provisions of the PDPA.

The Policy further provides an overview of the PDPA in respect of the statutory obligations imposed on the related companies of WPG South Asia Group. The key management and the employees of all the related companies of WPG South Asia Group are to implement the necessary actions within the functions under each personnel's purview in accordance with the Checklist of Actions as set forth under Appendix B of this Policy.

2.0 Personal Data Protection Act 2012

The PDPA sets out various rules governing the collection, use, disclosure and care of personal data. It serves to protect the rights and privacy of individuals as well as to allow them the rights of access and correction to their own personal data.

A Do-Not-Call ("DNC") Registry established under the PDPA provides a public platform for individuals to register their Singapore telephone numbers for the purpose of opting out from marketing calls, messages and faxes. An organisation is prohibited from making marketing calls, sending and faxing marketing messages to Singapore telephone numbers registered with the DNC Registry unless a clear and unambiguous consent is obtained from the individual.

"Personal Data" is defined to include data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access. This includes, for example: full name, NRIC number, passport number, photograph or video images, mobile telephone number, personal email address, thumbprint, DNA profile, residential address, residential phone number of an individual.

"Business Contact Information" is exlcuded from the coverage of the PDPA. Such Business Contact Information is defined as "an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purpose".

The PDPA imposes certain statutory obligations on an organisation in the managing of personal data. The guidelines on such statutory obligations will be explained in detail under Section 4.0 of this Policy.

3.0 Enforcement of the Policy

The PDPA regulates personal data collected, used, stored and disclosed within the territory of Singapore. Notwithstanding this, Section 26 of the PDPA governs the transfer of data outside Singapore. Where personal data is transferred ouside Singapore, the organisation shall ensure that the recipient(s) provide a comparable standard of protection as conferred by the PDPA.

Given this, all related companies under WPG South Asia Group as set forth in Appendix A annexed to this Policy (which may be updated from time to time), whether the company is located within or outside Singapore, shall observe the guidelines fully as set forth in this Policy.

Under the PDPA, the consequences of breach include taking remedial action(s) in respect of the data collected, used and/or disclosed as well as paying a financial penalty up to SGD 1 Million. For breach of duties in respect of the DNC Registry, an organisation shall be liable to a fine up to SGD 10,000.00 for each offence.

4.0 Statutory Obligations under the PDPA

The statutory obligations imposed on an organisation which collects, uses, stores and/or discloses personal data are as follows:

4.1 Consent Obligation

An organisation must obtain the consent of the individual before collecting, using or disclosing his personal data for a purpose.

4.2 Purpose Limitation Obligation

An organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and, if applicable, have been notified to the individual concerned.

4.3 Notification Obligation

An organisation must notify the individual of the purpose(s) for which it intends to collect, use or disclose the individual's personal data on or before such collection, use or disclosure of the personal data.

4.4 Access and Correction Obligation

An organisation must, upon request, (i) provide an individual with his or her personal data in the possession or under the control of the organisation and information about the ways in which the personal data may have been used or disclosed during the past year; and (ii) correct an error or omission in an individual's personal data that is in the possession or under the control of the organisation.

4.5 Accuracy Obligation

An organisation must make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete if the personal data is likely to be used by the organisation to make a decision that affects the individual concerned or disclosed by the organisation to another organisation.

4.6 Protection Obligation

An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

4.7 Retention Limitation Obligation

An organisation must cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that (i) the purpose for which the personal data was collected is no longer being served by retention of the personal data, and (ii) retention is no longer necessary for legal or business purposes.

4.8 Transfer Limitation Obligation

An organisation must not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA.

4.9 Openness Obligation

An organisation must implement the necessary policies and procedures in order to meet its obligations under the PDPA and shall make information about its policies and procedures publicly available.

5.0 Appointment of Data Protection Officer

An organisation is required to designate at least one (1) person as the Data Protection Officer for development of the organisation's policy and oversee the organisation's compliance with the PDPA, handling queries or complaints relating to the management of personal data as well as acting as the contact person for liaison with the PDPC where necessary.

The Data Protection Officer of WPG South Asia Group shall be the Legal Counsel in charge at the time being or any other personnel as appointed by WPG South Asia Group to assume the said position.

The contact information of the Data Protection Officer shall be made available in the Personal Data Protection Policy as published in the official website of WPG South Asia Group in accordance with the requirements of the PDPA.

APPENDIX A
LIST OF ENTITIES

(A) Singapore

1. WPG South Asia Pte Ltd
2. World Peace International Pte Ltd
3. World Peace International (South Asia) Pte Ltd
4. Genuine C&C (Indochina) Pte Ltd
5. SAC Components (South Asia) Pte Ltd
6. Yosun Singapore Pte Ltd
7. Richpower Electronic Devices Pte Ltd
8. Vitec WPG Limited (Singapore Branch)

(B) Malaysia

1. WPG Malaysia Sdn Bhd
2. WPG C&C (Malaysia) Sdn Bhd

(C) India

1. WPG India Electronics Private Limited
2. WPG C&C Computers & Peripheral (India) Private Limited
3. World Peace International (India) Private Limited
4. Yosun India Private Limited

(D) Thailand

1. WPG (Thailand) Co., Ltd
2. WPG C&C (Thailand) Co., Ltd

(E) Philippines

1. WPG Electronics Philippines Inc

(F) America

1. WPG Americas Inc

(G) Hong Kong

1. WPG SCM Limited

(H) Vietnam

1. WPG Vietnam Company Limited

APPENDIX B
CHECKLIST OF ACTIONS

No.	Checklist of Actions
1	**Submission of Record** All Managers are to collate the information required and send the Record according to the format set out in ***Appendix C*** to the Data Protection Officer for filing.
2	**Type of Personal Data** Identify the personal data collected from ***customers***, ***vendors***, ***employees***, ***candidates***, ***agents***, and ***representatives*** that are governed by the PDPA: a) Full name b) NRIC or FIN number c) Passport number d) Photograph or video image of an individual e) Mobile telephone number f) Personal email address g) Thumbprint / DNA profile h) Name and residential address i) Name and residential telephone number j) Any other information that may identify an individual
3	**Collection and Storing of Personal Data** Managing the collection and storing of personal data by keeping a record of the following within your department/ team (the "Record"): a) Identify the personnel within your department / team who collect personal data. Managers are to identify the personnel within the department/ team who are responsible in collecting personal data. To better manage the collection of personal data, managers may restrict access to such data to certain personnel within the department/ team. b) Identify the location where the personal data is stored. Managers are to assign a specific location (physical or electronic form) where all personal data collected are stored securely with restricted access. Network & Infrastructure Department and IT Department are to render assistance in providing proper electronic platforms for storing of personal data by the respective department/ team where required
4	**Consent of Individual** The PDPA requires that consent of the individual to be obtained for the purpose(s) for which the personal data will be collected, used or disclosed. a) Obtaining consent of the individual / Withdrawal of consent Managers are to ensure that the following acknowledgment column is incorporated into all documents that collect personal data from individuals. This statement further allows the individual to withdraw his/her consent at any time, in writing to the company.

	[ ] I hereby acknowledge and consent to any and all personal data submitted by me herein to be collected, used and disclosed by the Company for the purposes as conveyed to me by the relevant personnel of the Company or as outlined in the Company's Personal Data Protection as published in its official website. I understand that I may at anytime, withdraw this consent in writing to the Company. b) Engagement of Data Intermediary Data intermediary is a representative/agent that collects, uses or discloses personal data on behalf of a company. Managers that engage such data intermediary are to inform the Data Protection Officer for review of the scope of services and obligations of the data intermediary and to ensure that the data intermediary complies with the standard as prescribed by the PDPA.
5	**Use of Personal Data** a) Limitation on the use of personal data The use of personal data should be limited to the purposes that one has obtained consent for. For example, information submitted by a job applicant to the HR Department should only be limited for the purposes of interviewing, hiring the individual or for submission to the relevant government authority for statutory registration(s) required of an employee of a company. For personal data that is collected prior to the PDPA coming into force may continue to be used for the purposes for which the personal dta was collected, unless the individual has withdrawn consent to it. If there is a fresh purpose for the use of such personal data, consent should be obtained again from the individual.
6	**Disclosure of Personal Data** a) Limitation on the disclosure of personal data Managers should limit the disclosure of personal data collected to only purposes that one has obtained consent for. b) Identify the recipient of the personal data (where it is disclosed to). Personal data collected should not be released to any unauthorised third parties. Where required, consent of the individual should be obtained if his/her personal data is to be released.
7	**Access and Correction of Personal Data** a) Procedure to handle requests for access to personal data All requests in relation to access to personal data shall be submitted to the Data Protection Officer for review and assessment in accordance with the requirements and exceptions as provided under the PDPA. The approval or rejection of the request shall be provided by the Data Protection Officer, upon assessment of the same, within a reasonable time period, and in any event, no longer than five (5) working days from the date of the request. The Data Protection Officer may, subject to reasonable justification being provided, extend the time period as required in accordance with the Personal Data Protection Regulations 2014. b) Third party recipient of personal data In cases where the individual's personal data has been or may have been used or disclosed by the company within one (1) year before the request, such information shall, upon assessment by the Data Prtoection Officer, be made available to the individual within the same time period as

	provided for request of personal data. c) <u>Procedures to handle requests for correction requests of personal data</u> All requests in relation to correction of personal data shall be submitted to the Data Protection Officer for review and assessment together with any valid supporting documents in accordance with the requirements and exemptions as provided under the PDPA. The approval or rejection of the request shall be provided by the Data Protection Officer upon assessment of the same, within a reasonable time period, and in any event, no longer than five (5) working days from the date of the request.The personnel in charge of correcting the personal data shall within a reasonable time period, and in any event, no longer than five (5) working days from the date of approval given by the Data Protection Officer, make the necessary correction. The Data Protection Officer may, subject to reasonable justification being provided, extend the time period as required in accordance with the Personal Data Protection Regulations 2014. A confirmation in respect of the correction made to the personal data shall be sent to the individual in writing. The corrected personal data may, subject to the request and consent of the individual, be sent to every other organisation to which the personal data was disclosed by the company within one (1) year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose. d) The company reserves the right to charge a reasonable administrative fee for request made in relation to the individual's personal data in accordance with the Personal Data Protection Regulations 2014. Such administrative fee shall be made known to the individual prior to accepting and processing the request. The company shall not be obliged to accept and process any request where the individual is not agreeable to the administrative fee to be incurred.
8	**<u>Accuracy of Personal Data</u>** Managers are to ensure that reasonable effort is made to verify that the personal data kept are accurate and complete: (i) Prior to using it to make a decision that affects the individual; or (ii) Prior to disclosure to any other organisation. "Reasonable effort" in this context shall include verifying the personal data against any relevant documents provided by the individual or verify with the individual personally to ensure that the personal data collected are accurate and complete.
9	**<u>Protection of Personal Data</u>** a) <u>Deploying adequate security measures</u> Managers are to ensure that adequate security measures are deployed in the protection of personal data collected whether in physical or electronic forms. Network & Infrastructure Department and IT Department are to render assistance in providing adequate security measures for storing of personal data by the respective department/ team where required. b) <u>Classification of personal data</u> Different sets of personal data may be accessed by various parties (such as employees, vendors, agents and representatives). Managers are to ensure that the various parties access the personal data on a need-to-know basis, classified and stored adequately to ensure authorised access.

	c) Access by external third parties Where external third parties have unrestricted or easy access to the personal data stored, records of such access should be filed accordingly. Visitors to office premises shall be escorted and employees shall be informed prior to ensure that all personal data are kept securely and out of sight of the visitors. d) Regular audit and remedial actions The Data Protection Officer shall conduct audit on data protection processes and review adequacy of the compliance measures taken by the Managers on a regular basis. Remedial actions (if any) shall be presented to the Managers following the completion of the audit. Managers shall, within fifteen (15) days from the date of the audit report, carry out the remedial actions accordingly to ensure full compliance with the PDPA.
10	**Retention Limitation on Personal Data** a) Regular data housekeeping Managers shall not keep personal data for longer than the same is necessary for business or legal purposes. Retention period for various classification of personal shall be subject to the general guidelines as set forth below and may vary depeding on the nature of the personal data. Where required, the retention period of the personal data classified herein or not subject to the following classification shall be assessed by Managers and Data Protection Officer on a case-to-case basis: (i) Personal data of customers, vendors, agents and representatives with active and ongoing business dealings – Ongoing until the termination of contractual relationship and/or business dealings. (ii) Personal data of former customers, vendors, agents and representatives with no active and ongoing business dealings – No more than seven (7) years. (iii) Personal data of potential candidates for job application – No more than two (2) years. (iv) Personal data of current employees – Ongoing until the termination of employment and/or retirement of the employee. (v) Personal data of former employees – No more than seven (7) years. b) Removal of personal data Where such personal data exceeds the retention limitation period as set forth above, any physical or electronic records of the personal data shall be securely destroyed and/or anonymised to the extent where no individual shall be identifiable from the personal data stored.
11	**Cross Border Transfer of Personal Data** Where personal data is transferred ouside Singapore, the organisation shall ensure that the recipient(s) provide a comparable standard of protection as conferred by the PDPA. Given this, all related companies under WPG South Asia Group as set forth in Appendix A whether the company is located within or outside Singapore, shall observe the guidelines fully as set forth in this Policy.
12	**Openness Obligation**

	a) Appointment of Data Protection Officer This matter is dealt with under section 5.0 of this Policy. b) Publishing the terms and conditions of the Personal Data Protection Policy The terms and conditions of the Personal Data Protection Policy shall published in the official website of WPG South Asia Group in accordance with the requirements of the PDPA c) Communication to the employees This Policy shall be uploaded to the internal information sharing platform of WPG South Asia Group so as to ensure that all employees are adequately informed of the same.
13	**Do-Not-Call ("DNC") Registry** The DNC Registry provisions under the PDPA generally prohibits organisations from sending certain marketing messages to telephone numbers, including mobile, fixed-line, residential and business numbers, registered with the registry. If the individual has not given you his/her clear and unambiguous consent, evidenced in writing or any other accessible form, to the sending of the telemarketing messages to his /her telephone number, a thorough check on the DNC Register must be made prior to sending of such messages. The main duties of an organisation in respect of the DNC Registry include: a) Duty to check the DNC Registers Before a person sends a telemarketing message to a Singapore telephone number, the person must check with the DNC Registers established by the PDPC under the Act to confirm that the number is not listed on a DNC Register, unless the person has obtained clear and unambiguous consent in evidential form from the user or subscriber of the number (section 43 of the Act); and b) Duty to identify the sender of a message When sending a specified message to a Singapore telephone number, the person must: • include information identifying the sender and how the recipient may contact the sender; and • for voice calls, not conceal or withhold the sender's calling line/identity from the recipient .

APPENDIX C
FORM - MANAGEMENT OF PERSONAL DATA

FORM - MANAGEMENT OF PERSONAL DATA

1. Company: _____

2. Department / Division: _____

3. Staff Name: _____

4. Type of personal data collected:
(For ex: NRIC number of employees, contact number of customers, photographs taken during company events etc. Please refer to point 1 under "Appendix A - Checklist of Actions" for examples of personal data.)

_____
_____
_____
_____

5. Method of collection of personal data:
(For ex: By referral, direct collection from the individual etc.)

_____
_____
_____

6. Use of personal data:
(For ex: To conduct marketing calls, for submission to government authorities, for internal use etc.)

_____
_____
_____
_____

7. Storage location of personal data (physical or electronic forms):

_____
_____

8. Are the personal data disclosed to any third party not within your Department/Division?

[ ] Yes. Who? _____
[ ] No

REMINDER**: All Managers are reminded to review the "Checklist of Actions"*** as set forth in the Personal Data Protection Policy of WPG South Asia Group. Responsibility to ensure compliance with the statutory obligations as required by the Personal Data Protection Act rests with the respective Manager-in-charge of each Department / Division.

APPENDIX D
PERSONAL DATA PROTECTION POLICY (TERMS AND CONDITIONS)

(To be published in the official website of WPG South Asia Group)

PERSONAL DATA PROTECTION POLICY

1. This Personal Data Protection Policy sets out the terms and conditions relating to the collection, use and disclosure of personal data in accordance with the statutory requirements as set forth in the Personal Data Protection Act 2012 of Singapore (the "Policy").

2. This Policy shall apply to all related companies under the WPG South Asia Group (the "Company").

3. The term "Personal Data" is defined to include data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access.

4. By communicating and submitting Personal Data to the Company, you acknowledge, agree and consent to the Company in the collection, use and disclosure of the same in accordance with the terms and conditions set forth herein.

5. Colletion of Personal Data:

   Generally, the Company collects Personal Data from customers, prospective customers, suppliers, vendors, agents, representatives and third parties through the following methods:

   5.1 Submission of application forms any other documents relating to the goods and services offered by the Company;
   5.2 Communication with the employees, agents and/or representatives of the Company through telephone calls, emails, letters, text messages, face-to-face meetings or faxes;
   5.3 Accessing or utilising the websites, software applications or interactive and common sharing platforms established by the Company; and/or
   5.4 Receiving referrals from customers, prospective customers, suppliers, vendors, agents, representatives and third parties.

6. Purposes for the Collection, Use and Disclosure of Personal Data:

   The Company collects Personal Data from customers, prospective customers, suppliers, vendors, agents, representatives and third parties for purposes relating to the goods and services offered by the Company, including but not limited to:

   6.1 Attending to queries relating to the goods and services offered by the Company;
   6.2 Processing the purchasing orders submitted to the Company in respect of the goods and services offered by the Company;
   6.3 Attending to feedback and handling of complaints relating to the goods and services offered by the Company;
   6.4 Preparing transaction documents, purchase contracts, tax invoices and/or other documents relating to the goods and services offered by the Company;

6.5 Submission of shipping documents for delivery of the goods and services offered by the Company;
6.6 Providing customer service support in relation to the goods and services offered by the Company;
6.7 Conducting market research and survey; and/or
6.8 Processing job application within the Company.

7. Disclosure of Personal Data

Subject to the extent where permissible by the Personal Data Protection Act 2012, its regulations and other applicable laws, Personal Data may be disclosed by the Company for the abovementioned purposes to the following parties on a need-to-know basis:

7.1 Any customer, prospective customer, supplier, vendor, agent, representative and third party that may be relevant to the dealings between you and the Company or the goods and services offered;
7.2 the Company's professional advisors including but not limited to auditors and/or solicitors;
7.3 Any governmental authority, statutory board or enforcement agency for the purpose of compliance with any applicable laws, regulations, guidelines and/or schemes in force for the time being; and/or
7.4 Any other party whom you authorise the Company to disclose your Personal Data to.

8. Do-Not-Call (DNC) Registry

In line with the provisions relating to the Do-Not-Call (DNC) Registry, the Company will not send any telemarketing messages to Singapore registered telephone numbers that are registered on the DNC Registry through voice calls, text messages or faxes unless where you have given the Company your clear and unambiguous consent in writing to the Company. Such consent may be withdrawn by you at any time in writing to the Company.

9. Contact Information

You may contact the Company in writing for any other matters set forth below:

Data Protection Officer
WPG South Asia Group
10 Upper Aljunied Link #06-07,
Singapore 367904

9.1 You have any question or feedback relating to this Policy;
9.2 You have any question, feedback or complaint relating your Personal Data collected, used and/or diclosed by the Company;
9.3 You wish to withdraw your consent to any use of your Personal Data collected by the Company;
9.4 You wish to obtain access and/or request for correction of your Personal Data collected by the Company.