Data Protection Policy

1. Policy Statement

Every day our business will receive, use and store personal information about our Business Partners and colleagues. It is important that this information is handled lawfully and appropriately in line with the data protection requirements of the General Data Protection Regulation and Singapore Personal Data Protection Act.

We take our data protection duties seriously, because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

2. About This Policy

This policy, and any other documents referred to in it, sets out the basis on which we will process any personal data we collect or process.

This policy does not form part of any employee's contract of employment and may be amended at any time.

Roman C. Luth is responsible for ensuring compliance with the Data Protection Requirements and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer or reported in line with the organisation's Whistleblowing Policy.

3. What is Personal Data?

Personal data means data (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession).

Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes personal data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about criminal offences or convictions. Sensitive personal data can only be processed under strict conditions, including with the consent of the individual.

4. Data Protection Principles

Anyone processing personal data, must ensure that data is:

a. Processed fairly, lawfully and in a transparent manner
b. Collected for specified, explicit and legitimate purposes and any further processing is completed for a compatible purpose
c. Adequate, relevant and limited to what is necessary for the intended purposes
d. Accurate, and where necessary, kept up to date
e. Kept in a form which permits identification for no longer than necessary for the intended purposes
f. Processed in line with the individual's rights and in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
g. Not transferred to people or organizations situated in countries without adequate protection and without firstly having advised the individual (*unless stated in Clause 14 Disclosure and Sharing of Personal Data*)

5. Fair and Lawful Processing

The Data Protection Requirements are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individual.

In accordance with the Data Protection Requirements, we will only process personal data where it for our business needs and for a lawful purpose. The lawful purposes include (amongst others): whether the individual has given their consent, the processing is necessary for performing a contract with the individual, for compliance with a legal obligation, or for the legitimate interest of the business. When sensitive personal data is being processed, additional conditions must be met.

6. Processing for Limited Purposes

In the course of our business, we may collect and process the personal data. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, location data, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

We will only process personal data for our business needs or for any other purposes specifically permitted by the Data Protection Requirements. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

7. Marketing / Optional Purposes

To comply with Singapore Personal Data Protection Act – Do Not Call Provisions. We will check the DNC Register and identify sender.

From time to time, we may contact individual via mail, electronic mail, telephone (call or SMS-Text), facsimile or social media platforms, to inform them about our services and events that we think may be interest to them.
Individual can let us know at any time if they no longer wish to receive marketing materials and we will remove their details from our database.
Please note that we may still send individual non-marketing messages, customer-service notices and other service-related notices.

8. Notifying Individuals

If we collect personal data directly from an individual, we will inform them about:

a. The purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing
b. Where we rely upon the legitimate interests of the business to process personal data, the legitimate interests pursued
c. The types of third parties, if any, with which we will share or disclose that personal data
d. The fact that the business intends to transfer personal data to a non-EEA country or international organisation and the appropriate and suitable safeguards in place
e. How individuals can limit our use and disclosure of their personal data
f. Information about the period that their information will be stored or the criteria used to determine that period
g. Their right to request from us as the controller access to and rectification or erasure of personal data or restriction of processing
h. Their right to object to processing and their right to data portability
i. Their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn
j. The right to lodge a complaint with the Information Commissioners Office
k. Other sources where personal data regarding the individual originated from and whether it came from publicly accessible sources
l. Whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and any consequences of failure to provide the data
m. The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual

If we receive personal data about an individual from other sources, we will provide them with this information as soon as possible (in addition to telling them about the categories of personal data concerned)

We will also inform data subjects whose personal data we process that we are the data controller with regard to that data that our contact details are 8 EU TONG SEN STREET

#14-94, THE CENTRAL, SINGAPORE (059818).

9. Adequate, Relevant and Non-Excessive Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

10. Accurate Data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

11. Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

12. Processing in line with Data Subject's Rights

We will process all personal data in line with data subjects' rights, in particular their right to:

a. Confirmation as to whether or not personal data concerning the individual is being processed
b. Request access to any data held about them by a data controller (see also *Clause 15 Subject Access Requests*)
c. Request rectification, erasure or restriction on processing of their personal data.
d. Lodge a complaint with a supervisory authority
e. Data portability
f. Object to processing including for direct marketing
g. Not be subject to automated decision-making including profiling in certain circumstances

13. Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

We will put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to a data

processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

a. **Confidentiality** means that only people who are authorized to use the data can access it
b. **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed
c. **Availability** means that authorized users should be able to access the data if they need it for authorized purposes. Personal data should therefore be stored on the central computer system instead of individual PCs

Security procedures include:

a. **Entry controls.** Any stranger seen in entry-controlled areas should be reported
b. **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential)
c. **Data minimization**
d. **Pseudonymization and encryption of data**
e. **Methods of disposal.** Paper documents shall be shredded. Digital storage devices should be physically destroyed when they are no longer required
f. **Equipment.** Staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended

Transferring Personal Data under the Data Protection Act

We may transfer any personal data under the Data Protection Act we hold to a country outside of Singapore or to an international organisation, provided that one of the following conditions applies:

a. The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms
b. The data subject has given his consent
c. The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject
d. The transfer is legally required on important public interest grounds or for the establishment, exercise or defense of legal claims
e. The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights

Subject to the requirements above, personal data we hold may also be processed by staff operating outside Singapore who work for us or for one of our suppliers. Those staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

14. Disclosure and Sharing of Personal Data

We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as well as external organization for purposes mentioned before, subjected to the requirements of applicable laws:

a. A company subjected to a Collective Agreement with one of our affiliates
b. Agents, contractors, data intermediaries or third party service providers who provide services, such as telecommunications, mailing, information technology, payment, payroll, data processing, training, market research, carding, storage and archival, to the Organisation
c. External banks, financial institutions, credit card companies and their respective service providers
d. Our professional advisers such as our auditors
e. Relevant government regulators, statutory boards or authorities or law enforcement agencies to comply with any laws, rules, guidelines and regulations or schemes imposed by any government authority
f. Any other person in connection with the purposes set forth above

15. Subject Access Requests

Individuals must make a formal request for information we hold about them. Employees who receive a request shall forward it to the Data Protection Officer immediately.

When receiving telephone enquiries, we will suggest that the caller put their request in writing. Where a request is made electronically, data will be provided electronically where possible.

Our employees will refer a request to the Data Protection Officer for assistance in difficult situations.

16. Changes to this Policy

We reserve the right to change this policy at any time. Where appropriate, we will notify changes by mail or email.

Roman C. Luth
Data Protection Officer
01 January 2025