Personal Data Protection Act 2012

Personal Data Protection Policy

Visions.One Consulting Pte Ltd

Preamble

To our esteemed customers, business partners, contacts and employees

Ladies and gentlemen,

The processing of sales and marketing procedures via electronic means, the fast pace of globalization of our market space and reach and the coming into force of the Personal Data Protection Act 2012 ("PDPA") are together placing increased demands in the handling of personal data of or by our employees, service providers, customers and prospects, which we aim to meet.

As a responsible organisation, we aim to offer our employees, customers and business partners worldwide a high, uniform standard in the handling of their personal data. Careful data handling is in line with the expectations of our customers and business partners and forms the basis for a trusted business and employment relationship.

This corporate policy sets out our corporate personal data protection policy for the handling of personal data of our employees, prospects, customers and business partners, which is in conformity with the PDPA. It also sets out our policy for employees and internal staff, contractors to follow when handling personal data. All employees and staff working within our organisation should familiarize themselves with the contents of this policy and comply with its provisions.

Our Data Protection Officer, Ms Jamie Tan is responsible for making sure that the data protection guidelines and laws are implemented. She can be reached at 69666183 and support@visions1.com.sg. My staff and I would be happy to assist you with any questions you may have concerning data protection.

Mr James Leong
Chief Executive Officer
Visions.One Consulting Pte Ltd

Article 1: Personal Data Protection Policy

1.1 In this era of information technology, the value of personal data has become increasingly apparent. Virtually all transactions are processed electronically, and in the course of business, personal data inevitably changes hands. However, with the growing importance of personal data, the protection of such information has become an increasingly complex task. Further, the collection and processing of personal data is subject to a wide range of regulations, which demand immediate compliance.

1.2 Visions.One Consulting Pte Ltd (the "Firm") is committed to protecting the privacy and confidentiality of all personal data of its customers, employees and other individuals. The Firm recognises that a high standard of data security is needed to meet the expectations of our customers and the public, and to maintain a relationship of trust with our employees and business partners.

1.3 In line with this, the Firm has established this Personal Data Protection Policy (the "Policy"), which sets out the framework for the Firm's management of personal data. This Policy establishes a robust and comprehensive system, which serves to protect personal data within the Firm's control from unauthorised access and illegitimate use. This Policy is strictly enforced across the Firm, and reflects the Firm's dedication to maintaining the security and privacy of all personal data entrusted to the Firm.

1.4 Please note that the provisions of this Policy apply to the Firm's dealings and interaction with its employees, service-providers, contractors, consultants and customers ("Third Parties") in addition to the Firm's Privacy Policy (see www.visions1.com.sg) and the provisions of other policies of the Firm (insofar as they are stated to be so applicable) – all of which are to be read together as one document.

1.5 The Policy does not supersede nor replace any other consents which the Third Parties may have previously provided to the Firm nor does it affect any rights that the Firm may have at law in connection with the collection, use and/or disclosure of Third Parties' personal data. The Firm may from time to time update this Policy to ensure that this Policy is consistent with our future developments, industry trends and/or any changes in legal or regulatory requirements. If any material revision is made to this Policy, updates will be published at www.visions1.com.sg.

1.6 For the avoidance of doubt, this Policy forms a part of the terms and conditions governing the relationship between the Firm and Third Parties and should be read in conjunction with such terms and conditions ("Terms and Conditions"). In the event of any conflict or inconsistency between the provisions of this Policy and the Terms and Conditions, the provisions of the Terms and Conditions shall prevail.

1.7 Without prejudice to the generality of the Policy, please refer to the Firm's Privacy Policy (which can be found at www.visions1.com.sg for specific guidance on how the Firm collects, maintains and protects personal data of the Firm's customers particularly through the Firm's website.

1.8 In Singapore, the management of personal data is governed by the Personal Data Protection Act 2012 (the "PDPA"). In keeping with this, the Firm's collection, use, disclosure, and retention of personal data, as set out in this Policy, are in accordance with the PDPA. The application of the articles within this Policy is to be guided by the provisions and requirements of the PDPA, and any other written law.

Article 2: Objectives

2.1 The objectives of this Policy are as follows:

(a) To establish a framework for the responsible management of personal data;
(b) To ensure that all personal data and customer privacy is adequately protected;
(c) To facilitate customer and employee understanding of the Firm's personal data policy and processes, as well as provide channels for communication; and
(d) To ensure compliance with all provisions of the PDPA.

Article 3: Scope

3.1 In the course of business, the Firm may collect personal data from individuals, including:
(a) Clients and customers;
(b) Current, past, and prospective employees;
(c) Suppliers and contractors;
(d) Agents and consultants; and
(e) Members of the public.

3.2 This Policy applies to the management of all personal data controlled by the Firm including (save where otherwise provided in other documents or contracts, HR/staff handbooks issued by the Firm) personal data belonging to employees.

3.3 In this Policy, personal data refers to data from which an individual can be identified, and includes:
(a) An individual's name, NRIC, passport or other identification number, photograph, telephone number, mailing address, and email address;
(b) An individual's employment history, education background, and income levels;

3.4 This Policy does not apply to business contact information, where business contact information refers to data provided to the Firm for purposes that are

not solely personal. However, where it is unclear if the data collected or intended to be used constitutes business contact information, the Firm shall treat it as personal data to which this Policy shall apply.

Article 4: Consent

4.1 The Firm shall not collect, use, or disclose any individual's personal data without obtaining the individual's consent.

(a) The Firm shall not require an individual to consent to the collection, use, or disclosure of any personal data beyond what is reasonably necessary.

(b) The Firm shall not obtain an individual's consent using false information or misleading practices.

4.2 The Firm may also collect, use, or disclose personal data from an individual where he is deemed to have given his consent for such collection, or where required or authorised under the PDPA or any other written law. This includes instances where:

(a) The collection, use, or disclosure of the personal data is in the interest of the individual;

(b) The collection, use, or disclosure of the personal data is necessary in the national interest, or for any investigations of proceedings;

(c) The personal data is publicly available;

(d) The personal data is necessary for evaluative purposes; and

(e) The personal data is collected in the course of employment with the Firm and is reasonably necessary for purposes of managing or terminating the individual's employment.

4.3 For documentation purposes, statements of consent shall generally be obtained either in written or electronic form.

(a) In certain situations, consent may be given verbally, in which case the consent shall be properly documented.

(b) The statement of consent should indicate that the individual has been notified of the purpose for which the personal data will be collected, used, or disclosed.

Article 5: Collection of Personal Data

5.1 The Firm shall collect an individual's personal data only for purposes which a reasonable person would consider appropriate, and where the individual has been informed of and has consented to the purpose.

5.2 The Firm may collect personal data from customers and employees in the following ways:

(a) When an individual performs a transaction with the Firm;
(b) When an individual accesses the Firm's website;
(c) When an individual submits an application to the Firm;
(d) When an individual asks to be included in the Firm's mailing list;
(e) When an individual requests that the Firm contact the individual;
(f) When an individual responds to the Firm's promotions or requests for information; and
(g) When an individual submits his personal data to the Firm for any other reason.

5.3 Prior to obtaining consent for the collection of a person's personal data, the Firm or its employees shall seek to inform the individual of the following information:

(a) The identity of the collector of the personal data;
(b) The purpose for which the personal data is being collected;
(c) Any other purpose the personal data may be used for; and
(d) The third parties or categories of third parties to whom the personal data may be transferred.

Article 6: Storage of Personal Data

6.1 The Firm shall record all personal data in an accurate and complete manner.

6.2 The Firm shall make reasonable effort to ensure that all personal data is correct and up to date, particularly where:

(a) The personal data is likely to be used by the Firm to make a decision that affects the individual concerned; and

(b) The personal data is likely to be disclosed by the Firm to another organization.

6.3 All personal data collected by the Firm shall be stored in a secure and organised manner to prevent unauthorised access, loss, or modification.

(a) Personal data shall be treated as confidential, and shall only be accessible to authorised employees who require such data for the fulfillment of their duties, and only to the extent necessary for the scope of the task in question.

(b) Paper files and other physical documents containing personal data shall be kept in a secure environment.

(c) Personal data held on computers and computer systems shall be protected by appropriate software and technology.

(d) Where personal data is protected by password, such passwords shall be secure, private, and regularly changed, and shall not be shared or easily compromised.

(e) Personal data shall not be removed from the Firm, whether physically or electronically, unless absolutely necessary and with the requisite authorisation.

(f) The Firm shall implement formalised responses to any breach of security, whether by employees or by third parties.

Article 7: Use of Personal Data

7.1 The Firm shall use an individual's personal data only for purposes which a reasonable person would consider appropriate, and where the individual has been informed of and has consented to the purpose.

7.2 The Firm may use an individual's personal data for the following purposes:
(a) The provision of goods and services;
(b) The provision of customer service;
(c) The conduct of employee management;
(d) The fulfillment of any legal or regulatory requirement; or
(e) Any other legitimate business purpose.

7.3 Before accessing and using an individual's personal data, the Firm shall check the following:
(a) Whether the purpose for which the personal data is to be used has been consented to by the individual;
(b) Whether the individual's consent has been withdrawn, or is the subject of a withdrawal of consent request; and
(c) The extent to which the processing of the personal data is necessary for the intended purpose.

7.4 Where an individual has consented to having his personal data used for the contractual provision of goods and services:
(a) The personal data may be used for the purpose of executing the contract, such as for preparing offers, purchase orders, or fulfilling other customer requests;
(b) The Firm may contact the individual using his personal data for the purpose of the contract; and
(c) The personal data may be used for the provision of advisory services after the conclusion of the contract, provided it is consistent with the purpose of the contract.

7.5 Where an individual has consented to having his personal data used for the provision of customer service:

(a) The personal data may be used for the purpose of responding to the individual's requests, such as for replying to requests for information, or for fulfilling requests for access to personal information;
(b) The Firm may contact the individual using his personal data for the purpose of customer service; and
(c) The personal data may be used to follow up with the individual after the provision of customer service, provided it is consistent with the scope of the customer service.

7.6 Where an individual has consented to having his personal data used for advertising purposes:
(a) The personal data may be used to contact the individual for the provision of advertising material, such as through mail, e-mail, and telephone; and
(b) Employees of the Firm must ensure compliance with the terms of the Do Not Call Registry (see Article 14).

7.7 Where an individual has consented to having his personal data used for the conduct of employee management:
(a) The personal data may be used to contact the individual where the individual is an applicant to the Firm in order to respond to his application; and
(b) The personal data may be used for the purpose of employee management where the individual is an employee, such as for Human Resource related matters, or for security purposes.

7.8 Where the use of the personal data is otherwise authorised or required under the PDPA or any other written law:
(a) The Firm shall first ascertain that the use of the personal data is in fact authorised or required, such as in the national interest, in the individual's interest, or in for the purpose of investigations; and
(b) The Firm shall only process the personal data to the extent permitted or required, and in compliance with the relevant statutes or regulations.

7.9 All use and processing of personal data shall be conducted in an organised and secure manner.

(a) Personal data shall only be processed by authorised employees who have received adequate training in the proper management of personal data.

(b) Personal data shall be processed in accordance with formalised procedural guidelines for the management and handling of personal data.

(c) Personal data shall be kept private and confidential throughout processing.

Article 8: Transmission of Personal Data

8.1 In the course of business, it may be necessary for the Firm to disclose or transmit personal data, both within the organisation and to third parties.

8.2 The Firm shall disclose an individual's personal data only for purposes which a reasonable person would consider appropriate, and where the individual has been informed of and has consented to the purpose.

8.3 Before transmitting an individual's personal data, the Firm shall check the following:

(a) Whether the purpose for which the personal data is to be transmitted has been consented to by the individual;

(b) The extent to which the processing of the personal data is necessary for the intended purpose; and

(c) Whether the transmission is in conflict with any interest of the individual that merits protection.

8.4 If the personal data is to be transmitted to a recipient outside of Singapore, the Firm shall:

(a) Obtain sufficient contractual guarantee that the personal data shall be subject to a level of data protection in line with this Policy; or

(b) Otherwise ensure that the personal data shall be managed in accordance with the requirements of the PDPA.

8.5 It must be remembered that if the personal data is transmitted to a third party service provider for the purposes of processing, the security of the personal data remains the responsibility of the Firm. When selecting a third party service provider, the Firm shall thus ensure that:

(a) The service provider is capable of guaranteeing the necessary technical and organisational requirements to adequately protect the personal data;

(b) The service provider shall only process the personal data in accordance with the Firm's instructions; and

(c) The service provider's compliance with the data protection and information security requirements shall be included in its contract with the Firm.

8.6 In the case that personal data is transmitted to the Firm by a third party, the Firm shall ensure that:

(a) The data has been collected lawfully in accordance with the relevant legal provisions; and

(b) The individual has consented to the transmission and use of his personal data for the intended purpose.

8.7 All transmission of personal data shall be conducted in an organised and secure manner.

(a) Personal data shall only be transmitted by authorised employees who have received adequate training in the proper transmission of personal data.

(b) Personal data shall be transmitted in accordance with formalised procedural guidelines for the transmission and disclosure of personal data.

(c) Personal data shall be kept private and confidential throughout transmission.

Article 9: Retention

9.1 The Firm shall not keep personal data indefinitely. The Firm shall cease to retain personal data when:

(a) The purpose for which the personal data was collected is no longer being served; or

(b) Retention is no longer necessary for business or legal purposes.

9.2 [Personal data shall be retained for periods as follows:

(a) Personal data of customers: 7 years

(b) Personal data of employees: 7 years.

(c) The Firm may retain personal data beyond these periods where reasonable under the PDPA, or where required under any other written law.

9.3 When the Firm ceases to retain any personal data, such personal data shall be removed or deleted in a secure and permanent manner, or else properly anonymised to prevent further use.

9.4 Deletion or anonymisation of personal data shall be conducted in an organised and secure manner.

(a) Personal data shall only be deleted or anonymised by authorised employees who have received adequate training in the proper deletion or anonymisation of personal data.

(b) Personal data shall be deleted or anonymised in accordance with formalised procedural guidelines for the transmission and disclosure of personal data.

(c) Personal data shall be kept private and confidential throughout deletion or anonymisation.

Article 10: Personal Data Requests

10.1 An individual may request to be provided with all personal data about that individual that is within the Firm's possession, as well as information about how that data has been used or disclosed within a year before the request.

(a) Individuals may submit an **Access Request Form** to Ms Jamie Tan at support@visions1.com.sg
(b) The Firm shall endeavour to attend to all requests within 30 days, or within a period which is reasonable under the circumstances.
(c) The Firm shall not accede to a request where the provision of such data or information is not authorised or required under the PDPA or any other written law, or where the request is frivolous, vexatious, or may cause unreasonable interference with the Firm's operations.
(d) The Firm may charge a fee of S$10 for the cost and time of attending to the access request provided that such a charge has been clearly notified to the individual making the request.

10.2 An individual may request the Firm to correct an error or omission in his personal data that is within the Firm's possession.
(a) Individuals may submit a **Correction Request Form** to Ms Jamie Tan at support@visions1.com.sg
(b) The Firm shall endeavour to attend to all requests within 30 days, or within a period which is reasonable under the circumstances.
(c) The Firm shall correct the personal data as soon as practicable, and shall, where necessary, send the corrected personal data to any organisation the data was disclosed to within a year before the request.
(d) The Firm shall not accede to a request where the correction is not authorised or required under the PDPA or any other written law, or where there are reasonable grounds why the correction should not be made.

10.3 An individual may withdraw consent to the collection, use, or disclosure of his personal data upon the provision of reasonable notice to the Firm.
(a) Individuals may submit the **Withdrawal of Consent Form** to Ms Jamie Tan at support@visions1.com.sg

(a) The Firm shall endeavour to attend to all requests within 30 days, or within a period which is reasonable under the circumstances.

(b) The Firm shall notify the individual of the consequences of withdrawal of consent, and shall cease to collect, use, or disclose the individual's personal information upon processing of the notice of withdrawal within 30 days.

Article 11: Complaints & Queries

11.1 An individual may submit a complaint or query to the Firm regarding the application of this Policy and the PDPA, or any other issue related to the Firm's management of personal data.

(a) Individuals may object to their personal data being used for certain purposes, or may request that his personal data be deleted.

(b) Individuals may submit a **Complaints & Queries Form** to Ms Jamie Tan at support@visions1.com.sg

(c) The Firm shall endeavour to attend to all complaints and queries within 30 days, or within a period which is reasonable under the circumstances.

11.2 The Firm shall treat all complaints and queries seriously, and shall respond in an appropriate manner.

(a) All complaints and queries should be directed to the Ms Jamie Tan.

(b) The Firm's legal obligations under the PDPA and any other written law must be taken into account before any response to a complaint or query is given.

(c) When communicating directly with an individual expressing a complaint or query, employees shall respond in a polite and helpful manner.

(d) When responding to a complaint or query, employees shall provide the individual with a copy of this Policy, as well as the **Complaints & Queries Form.**

(e) All complaints and queries, as well as the responses given to the individual, shall be recorded and reported to the Ms Jamie Tan.

(f) Ms Jamie Tan shall periodically review the complaints and queries submitted to the Firm and take appropriate action to remedy any outstanding issues regarding the Firm's management of personal data.

Article 12: Compliance

12.1 The Firm shall protect the security of all personal data in its possession by making appropriate technical and organisational arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, and disposal.

12.2 The Firm shall ensure that:

(a) A adequate system of software and technology is in place to protect the security of all personal data, and that such system is periodically updated to ensure it is up-to-date;

(b) All personal data is kept physically secure through adequate security measures;

(c) A proper organisational plan is in place specifying the employees who are required to deal with personal data in the course of their duties and are thus authorised to access personal data;

(d) Formalised procedural guidelines for the collection, use, and disclosure of personal data are in place;

(e) All employees managing and handling personal data are appropriately trained and supervised;

(f) A regular review and audit is made of the manner in which personal data is managed;

(g) The Firm's data protection Policy and procedural guidelines are regularly revised in accordance with technological developments, organisational changes, and changes in the law; and

(h) The Firm's data protection Policy and procedural guidelines are strictly enforced.

12.3 All employees shall receive adequate and regular training in data protection. In keeping with this, all employees shall:

(a) Be provided with this Policy upon joining the Firm;

(b) Be regularly updated on and given access to this Policy;

(c) Be made aware of the requirements of the PDPA;
(d) Be made aware of the formalised procedural guidelines for the collection, use, and disclosure of personal data;
(e) Be briefed on the importance of maintaining the privacy and confidentiality of personal data
(f) Be made familiar with their role in maintaining the security of all personal data in the Firm's control;
(g) Be made aware that any unauthorised access of personal data, disclosure of personal data to unauthorised persons, and use of personal data for private or commercial purposes is strictly prohibited;
(h) Have adequate recourse, whether to their superiors or to the Data Protection Officer, for any queries on personal data; and
(i) Be trained in how to handle queries from the public on personal data.

12.4 All employees shall be required and trained to:
(a) Fully observe all legal and Policy requirements for the collection, use and disclosure of personal data;
(b) Ensure the quality of personal data used;
(c) Apply checks to determine the length of time personal data is held;
(d) Ensure that the rights of individuals about whom personal data is held can be fully exercised.

Article 13: Data Protection Officer

13.1 The Firm shall appoint a Data Protection Officer to supervise the observance of this Policy and all data protection requirements.
(a) The Data Protection Officer shall be appointed by Mr James Leong who shall have overall supervision of his/her responsibilities.
(b) The Data Protection Officer shall carry out his/her duties internally independent of professional orders where such orders run contrary to this Policy or the Personal Data Protection Act.
(c) The Data Protection Officer may appoint data protection coordinators within the various departments and business groups of the Firm.

(d) The Firm shall support the Data Protection Officer in his/her activities regarding the protection of personal data.

13.2 The Data Protection Officer shall:

(a) Be responsible for the general administration of the privacy and security of all personal data within the Firm's possession;
(b) Attend to the enforcement and implementation of this Policy;
(c) Ensure that employees are familiar with the content of this Policy and obtain the necessary training in data protection;
(d) Ensure compliance with this Policy and with the PDPA;
(e) Carry out data protection checks and audits;
(f) Be immediately informed of and respond to any data protection breaches;
(g) Be available to advise any employee on any data protection issue; and
(h) Be available to respond to any public queries, complaints, and requests for information regarding this Policy or any data protection issue.

13.3 Contact details for the Data Protection Officer are as follows:

Jamie Tan
Vice President, Operations
Tel: 69666183
support@visions1.com.sg

Article 14: Do Not Call Registry

14.1 The Firm shall not send marketing messages to Singapore telephone numbers without first checking and confirming that the telephone number is not listed on the Do Not Call Register, unless the individual has given consent to receive such messages.

14.2 The Firm shall not send marketing messages to Singapore telephone numbers without providing information identifying the sender and how to contact the sender.

14.3 The Firm shall not make voice calls to any Singapore telephone number concealing the identity of the caller from the recipient.

14.4 An individual who does not wish to receive such marketing messages may withdraw his consent upon the provision of reasonable notice to the Firm.