	Document Title	PERSONAL DATA PROTECTION ACT (PDPA) POLICY
	Version	1.0
	Effective Date	1 st November 2024
	Process Owner	HUMAN RESOURCE DEPARTMENT

INTRODUCTION

As part of **VSD Automation Sdn. Bhd. ("the Company")** and its related subsidiaries commitment to act with integrity and respect others, we protect the personal data of our stakeholders, including employees, customers, shareholders, partners, suppliers and other individuals who trust us with information.

"Personal data" includes information in respect of commercial transactions which identifies or locates an individual or is capable of doing so.

To be a trusted business partner, the Company continually strives to protect personal data in accordance with applicable laws and regulations, namely the data protection principles under the Personal Data Protection Act 2010. To that end, this policy guides how the Company collects, uses, stores, transfers and secures personal data and to ensure the rights of the data subjects are protected.

In this policy, the Company seek to inform data subjects of the purpose for which their personal data is collected and processed and the data subject's right to access or refuse to provide such personal data.

POLICY STATEMENT


Everyone has rights with regard to how their personal information is handled. During the course of the Group's activities the Company may collect, store and process personal information about staff, customers, suppliers, vendors, and the Company recognises the need to treat this data in an appropriate and lawful manner. the Company is committed to complying with its obligations in this regard in respect of all personal data it handles.

The types of information that the Company may be required to handle include details of current, past and prospective employees, suppliers, customers, and others that the Group communicates with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Personal Data Protection Act 2010 ('the Acts') and other regulations. The Acts impose restrictions on how the Company may collect and process that data.

This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action up to and including dismissal on any the Company employees.

PURPOSE AND SCOPE OF THE POLICY

This policy sets out the Company rules on data protection and the legal conditions that must be satisfied in relation to the collecting, obtaining, handling, processing, storage, transportation and destruction of personal and sensitive information.

	Document Title	PERSONAL DATA PROTECTION ACT (PDPA) POLICY
	Version	1.0
	Effective Date	1 st November 2024
	Process Owner	HUMAN RESOURCE DEPARTMENT

If an employee considers that the policy has not been followed in respect of personal data about themselves or others they should raise the matter with their manager as soon as possible.

DEFINITION OF DATA PROTECTION TERMS

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems. This would include IT systems and CCTV systems.

Data subjects for the purpose of this policy include all living individuals about whom the Company holds personal data.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information that is in, or is likely to come into, the possession of the data controller). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).


Data controllers are the individual or organisations who control and are responsible for the keeping and use of data.

Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following METRONIC's data protection and security policies at all times.

Processing means performing any operation or set of operations on data, including:

- obtaining, recording or keeping data,
- collecting, organising, storing, altering or adapting the data,
- retrieving, consulting or using the data,
- disclosing the information or data by transmitting, disseminating or otherwise making it available,
- aligning, combining, blocking, erasing or destroying the data.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, criminal convictions or the alleged commission of an offence. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

	Document Title	PERSONAL DATA PROTECTION ACT (PDPA) POLICY
	Version	1.0
	Effective Date	1 st November 2024
	Process Owner	HUMAN RESOURCE DEPARTMENT

DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the seven enforceable principles of good practice, namely:

- the General Principle;
- the Notice and Choice Principle;
- the Disclosure Principle;
- the Security Principle;
- the Retention Principle;
- the Data Integrity Principle; and
- the Access Principle.

As stated below.


GENERAL PRINCIPLE

The data subject must be told who the data controller is, the purpose for which the data is to be processed by the Group, and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, the Company shall ensure that all conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

The nature and type of data the Company collects and the source of such data varies depending on the nature of the relationship the Group has with the data subject and may include:

- personal data which the Company collects from its website, if such data has been voluntarily provided or where such data is required for the purposes of providing the service which a data subject requires
- personal data which we collect on application forms or other information forms such as name, address, email, telephone, occupation, income
- personal data from trade associations, marketing agencies, credit bureau reports and credit reporting agencies
- personal data from governmental agencies.

	Document Title	PERSONAL DATA PROTECTION ACT (PDPA) POLICY
	Version	1.0
	Effective Date	1 st November 2024
	Process Owner	HUMAN RESOURCE DEPARTMENT

Personal data is used to provide products and services and to inform about products and services offered by the Company and may include:

- profiling and determining service and supply preferences
- for the purposes of technical administration of the Company website
- statistical analysis
- developing new products and services
- registration for programs or offers upon the Company request
- providing goods and services offered to customers and consumers
- payment processing for purchases
- job application for employee recruitment
- protection against or identifying possible fraudulent transactions
- developing and providing advertising adapted to our customers
- finance and marketing operations and/or as required by the terms and conditions of business and other business administration purposes including credit monitoring and control purposes
- to meet regulatory and legal requirements
- for risk management
- for all other purposes incidental and associated with the above.

NOTICE AND CHOICE PRINCIPLE

The Company is aware that data subjects have the right to make a choice not to provide their personal data and may revoke their consent to the collection and processing of personal data. In this regard, the Company is aware that certain services it provides, and the continuation thereof may require the processing of such data. Failure to process such data may result in discontinuation of such services.

DISCLOSURE PRINCIPLE

Personal data should only be collected to the extent that it is required for any of the specific purposes stated in 6.4 which should be duly notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place. Personal Data will be kept confidential but may be disclosed to the following categories of parties for the purposes set out:

- to any companies in and outside of Malaysia
- to our advisers, including consultants, advocates and solicitors for purposes of determining our rights and enforcing any agreement with data subjects
- any agent, contractor or service provider to whom we may have outsourced services to, subject always that such parties acknowledge the confidentiality and rights of the data user and to comply with the provisions of the Act
- to regulatory authorities or notified bodies including bodies providing quality certification of our products upon their request
- to such other parties as may be permitted under Malaysian law.



Document Title	PERSONAL DATA PROTECTION ACT (PDPA) POLICY
Version	1.0
Effective Date	1 st November 2024
Process Owner	HUMAN RESOURCE DEPARTMENT

SECURITY PRINCIPLE

The Company and its employees must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.


The Acts require the Company to put in place procedures and technologies to maintain the security of all personal data. Personal data may only be transferred to a third-party data processor if the third party has agreed to comply with those procedures and policies or has adequate security measures in place.

The Company and its data users must demonstrate and put into practice the following core values to ensure:

- a) Confidentiality - that only people who are authorised to use the data can access it. the Company will ensure that only authorised persons have access to an employee's personnel file and any other personal or sensitive data held by the Group. Employees are required to maintain the confidentiality of any data to which they have access.
- b) Integrity - that the personal data is accurate and suitable for the purpose for which it is processed.
- c) Availability - that authorised users should be able to access the data if they need it for authorised purposes.

Security procedures to be put in place within the Company include:

- a) Secure workplace, 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.). Access rights to workplace are restricted to employees after office hours.
- b) Methods of disposal. Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.
- c) Equipment. Data users should 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.

	Document Title	PERSONAL DATA PROTECTION ACT (PDPA) POLICY
	Version	1.0
	Effective Date	1 st November 2024
	Process Owner	HUMAN RESOURCE DEPARTMENT

RETENTION PRINCIPLE

Data Subject's personal data shall be stored either in hard copies in the Group's offices or stored in servers located in or outside Malaysia and operated by the Group or its service providers in or outside Malaysia. Any personal data supplied to the Company will be retained by the Group as long as necessary for the fulfilment of the purposes stated in 6.4 above or to protect the Group's interests. The Company currently does not offer any online facilities for data subject to delete their personal data.

It shall be the duty of a data user to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed of which the method of disposal is stated in 9.4(b).

DATA INTERGRITY PRINCIPLE


Personal data must be accurate, complete, not misleading and kept up to date. Information which is incorrect or misleading is not accurate and steps should be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed. Employees should ensure that they notify their manager/Human Resources of any relevant changes to their personal information so that it can be updated and maintained accurately. Examples of relevant changes to data would include a change of address.

ACCESS PRINCIPLE

Data subjects including employees may request access to and correct their personal data held by the Company. If they wish to obtain a copy of any of their personal data; if they believe that the personal data relating to their which the Company collect and maintain is incorrect; or if they believe that the personal data held by the Company was used beyond the scope of the purposes described in 6.4 or was acquired by fraudulent or unlawful means or provided to a third party without their prior consent, data subjects may write to the Company at the addresses below.

A request for access or correction to, or deletion of personal data or for information regarding policies and practices and kinds of personal data held by the Company must be in writing and sent to the Company via (hr@vsdautomation.com)

The Company may charge a reasonable fee for the processing of any data access request(s).

	Document Title	PERSONAL DATA PROTECTION ACT (PDPA) POLICY
	Version	1.0
	Effective Date	1 st November 2024
	Process Owner	HUMAN RESOURCE DEPARTMENT

REVIEW OF POLICY

The Company will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives on at least every three years or more frequently if required taking into account changes in the law and organisational or security changes.

TRANSFERRING DATA OUTSIDE MALAYSIA

As the Company operates internationally, it may be necessary in the course of business that the Company has to transfer an employee's personnel data within the organisation and/or to other group companies to APACS country that is outside Malaysia, which do not necessary have comparable data protection laws to Malaysia. The transfer of such data is necessary for the management and administration of the contracts of employment and to facilitate Human Resources administration within the group. When this is required, the Company will take steps to ensure that the data has the same level of protection as it does inside of Malaysia.