



AL-Nasry @ Sengkang South Pte Ltd

Data Protection Policy

Version 1.1
24 January 2022

AL-Nasry Data Protection Policy

Key details

- Policy prepared by: Ismail Kay Jianming
- Reviewed by board / management on: Eugene Peh
- Policy became operational on: 27 September 2021
- Next review date: 03 January 2023
- Review approved by:

Change History Log

S/N	Version	Release Date	Updated By	Summary of Changes	Reviewed By	Approved By
1	1.0	27/09/2021	Affinite Solutions Pte Ltd (Ismail)	Initial release for operational	Affinite Solutions Pte Ltd (Eugene)	AL-Nasry @ Sengkang South Pte Ltd (Adlee)
2	1.1	24/01/2022	Affinite Solutions Pte Ltd (Eugene)	Update of Data breach Notification; Page 19	AL-Nasry @ Sengkang South (Siti Zuhra)	AL-Nasry @ Sengkang South (Adlee)

Contents

1. Objective	4
2. Scope	4
3. Personal Data of Children.....	5
4. Personal Data Protection Act	5
5. Data Protection Responsibilities	5
6. General staff guidelines	6
7. Collection of Personal Data	7
8. Use of Personal Data.....	9
9. Disclosure of Personal Data.....	10
10. On-going Notifications	11
11. Use of Cookies and Related Technologies	12
12. Data Protection Measures.....	13
13. Data storage.....	14
14. Data accuracy.....	15
15. Access & Correction Requests.....	15
16. Withdrawal of Consent	16
17. Retention of Personal Data.....	16
18. Transfers of Personal Data Outside Of Singapore.....	17
19. Data Protection Officer	17
20. Effect of Notice And Changes To Notice	17
21. Governing Law	17
22. Data Breach Management Plan.....	18

1. Objective

The Company is engaged in the business of Education.

In the course of conducting its business and providing the Programs listed below, the Company needs to gather and process personal data.

Programs:

- Integrated learning
- Raising readers for Life : Reading Aloud
- Life Long learners
- Developing creative and independent learners
- Fostering team spirit.
- Culture of Improving Practice
- Start Small Dream Big – Fundraising challenge

Learning Domains:

- Language and Literacy (English & Malay)
- Aesthetics and Creative expression
- Numeracy
- Discovery of the world
- Motor Skills Development
- Self and Social Awareness
- Projects
- Other Activities
- Values in Education

These can include personal data (any information that can or will lead to identifying you) from customers, suppliers, business contacts, employees, representatives, partners, agencies, authorities, contracting parties, III parties, and other individuals the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, used, disclosed, stored, protected to meet the Company's data protection standards and to comply with the Personal Data Protection Act 2012 of Singapore (PDPA).

The contents of this policy may be updated from time to time and individuals providing personal data should revisit this policy at least once every quarter.

This Policy is available on request. A version of this statement is also available on the Company's website.

2. Scope

This data protection policy ensures the Company:

- Complies with PDPA and follow good practices
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

3. Personal Data of Children

As our site is designed for parents and adults, we do not knowingly collect personal data from children who may visit our site, and we do not knowingly include any such information in our customer databases.

4. Personal Data Protection Act

PDPA describes how organisations must collect, use, disclose, and store personal data. Data protection includes collection, use, disclosure, and storage of personal data of individuals dealing with the Company.

The policy applies regardless of whether data is stored electronically, on paper, or on any other medium.

PDPA is underpinned by 11 key obligations (Whether in force or to be notified). According to these obligations, personal data must:

1. Be obtained with consent
2. Be obtained only for specific, lawful purposes
3. Be obtained with notification of purpose
4. Be provided for access and/or correction on request by applicant
5. Be accurate, up to date, adequate, relevant and not excessive
6. Be notified to relevant authorities and persons in the event of qualifying as a notifiable data breach
7. Be ported to another organization or platform on request
8. Be protected in appropriate ways
9. Not be retained or held for any longer than necessary
10. Not be transferred outside Singapore, unless that recipient country or territory or recipient organization also ensures an adequate level of protection
11. Be processed in accordance with requisite policies and practices, complaint handling process, and PDPA regulations
12. Be in compliance with Do Not Call (DNC) provisions

5. Data Protection Responsibilities

Everyone who works for or with the Company has relevant responsibility for ensuring data is collected, used, disclosed, stored and handled / processed appropriately.

These following people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that the Company meets its legal obligations
- The **[data protection officer]** (DPO) contact particulars are:

Name:	
-------	--

Email:	enquiries@alnasry.sg
Call:	+65 6489 6764
Write in:	Data Protection Officer 551 Hougang Street 51, #B1-296, Singapore 530552

- The DPO is responsible for the following:
 - i. Keeping the board updated about data protection responsibilities, risks and issues
 - ii. Reviewing all data protection procedures and related policies, in line with an agreed schedule
 - iii. Arranging data protection training and advice for the people covered by this policy
 - iv. Handling data protection questions from staff and anyone else covered by this policy
 - v. Dealing with requests from individuals to see the data the Company holds about them
 - vi. Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data

6. General staff guidelines

- i. The only people able to access data covered by this policy would be those who **need it for their work**
- ii. Data **is not shared informally**. When access to confidential information is required within the Company, employees will request it from their line managers
- iii. **The Company has and shall continue to provide training** to all employees to help them understand their responsibilities when handling data
- iv. Employees will **keep all data secure**, by taking sensible precautions and following the guidelines below:
 - In particular, **using strong passwords** and never be shared
 - Personal data **will not be disclosed** to unauthorised persons, either within the company or externally.
 - Data will be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it will be deleted and disposed of.
 - Employees **shall request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

7. Collection of Personal Data

By interacting with, submitting information to, or signing up with us for [any products or services] offered by us, you agree and consent to the Company (including their related corporations and overseas branches and offices) (collectively, the "Company"), as well as their respective representatives and/or agents ("Representatives") (the Company and Representatives are collectively referred to herein as "us", "we", or "our") collecting, using, disclosing and sharing amongst themselves your Personal data, and disclosing such Personal data to the Company's authorised service providers and relevant third parties in the manner set forth in this Data Protection Policy.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of PDPA.

We only collect data necessary for fulfilling our product / service requirements. By submitting you data, you are deemed to have given your consent to our collection, use, disclosure, and storage of your personal data. Please let us know if you wish to withdraw or vary your consent. In the event any other use of your personal data is contemplated, we will notify you of the same.

- a. Personal data may be collected in the following ways:
 - i. Form submission, including but not limited to application forms or other forms relating to any of our products or services which may be enquired about or purchased through the Company
 - ii. Any agreement or providing of other documentation or information in respect of your interactions with us, or when you use our services
 - iii. Interaction with our staff, including relationship managers and their assistants, example via telephone calls (which may be recorded), letters, fax, face-to-face meetings and emails
 - iv. Images captured via closed-circuit television cameras ("CCTVs") while you are within our premises, or via photographs or videos taken by us or our representatives when you attend events hosted by us
 - v. Use of services provided through our online and other technology platforms, such as websites and apps, including when you establish any online accounts with us
 - vi. Request that we contact you, or include you in an email or other mailing list; or when you respond to our request for additional personal data, our promotions and other initiatives
 - vii. Contact by, and / or response to, our marketing representatives, agents and other service providers
 - viii. Information sought about you and receipt of your personal data from third parties in connection with your relationship with us, for example, from referrers, business partners, external or independent asset managers, public agencies or the relevant authorities

- ix. Personal data through physical access, internet and information technology monitoring processes
 - x. Personal data in connection with any investigation, litigation, registration or professional disciplinary matter, criminal prosecution, inquest or inquiry which may relate to you
 - xi. Direct submission by you of your personal data to us
 - xii. Consent for any notification of new purposes
- b. The Company need not collect your consent under the following circumstances. Where collection of personal data:
- i. For legal purpose such as compliance with regulations under ECDA, IRAS, MOH, and all other relevant laws of Singapore
 - ii. Cannot be obtained in timely way
 - iii. Not reasonably be expected to withhold consent
 - iv. Is an emergency that threatens the life, health, or safety of the individual or another individual
 - v. The Company has reasonable grounds to believe that the health or safety of the individual or another individual will be seriously affected
 - vi. For the purpose of contacting the next-of-kin or a friend of any injured, ill or deceased individual
 - vii. Is publicly available
 - viii. Is in national interest
 - ix. For artistic or literary purposes
 - x. For archival or historical purposes (not for sensitive data)
 - xi. There is legitimate interest
 - xii. For business asset transactions
 - xiii. For business improvement purposes
- c. When you browse our website and platforms, you generally do so anonymously but please see the section below on cookies. We do not, at our website and platforms, automatically collect personal data, including your email address unless you provide such information or login with your account credentials.
- d. If you provide us with any personal data relating to a third party (for example, information of your spouse, children, parents, or a representatives), by submitting such information to us, you represent to us that you have obtained the consent of the third party to you providing us with his/her personal data for the respective purposes.

- e. Withdrawal of Consent: Should you wish to withdraw your consent for collection, use, or disclosure of your personal data, please contact the Company for such withdrawal of your personal data via the Personal Data Application Form (write in to our DPO to receive a copy of this form).
- f. In the event of missing field(s) or missing signature(s) from various forms, it will be deemed as incomplete registration. You may choose to complete the registration. If you choose to not proceed, no information will be registered in our system.
- g. Accuracy: You should ensure and check that all personal data submitted to us is complete, accurate, true, and correct. Failure on your part to do so may result in our inability to provide you with products and services you have requested. You agree to inform us immediately of any change of facts or circumstances which may render any information or personal data previously provided inaccurate, untrue, or incorrect and provide any information or documentation as we may reasonably require for the purposes of verifying the accuracy of the updated information or personal data.

8. Use of Personal Data

Personal data is of no value to the Company unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft. The general staff guidelines are:

- When working with personal data, employees to ensure **the screens of their computers are always locked** when left unattended.
- Personal data is **not shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of Singapore** unless recipient country and / or recipient organization observes personal data protection through law and policies. (Transfer Limitation)
- Employees **should not save copies of personal data to their own devices**. Always access and update the central copy of any data.

The Company hereby notifies you of use your personal data for the following purposes:

- a. verifying your identity
- b. managing the administrative and business operations of the Company and complying with internal policies and procedures and sharing between departments within the Company (including but not limited to facilitating business continuity planning)
- c. audit purposes
- d. verifying or confirming trade orders and transactions or instructions from you or for your orders

- e. facilitating business asset transactions (which may extend to any mergers, acquisitions or asset sales) involving the Company
- f. matching any personal data held which relates to you for any of the purposes listed herein
- g. responding to and resolving complaints and handling requests and enquiries, requests, feedback, and suggestions
- h. preventing, detecting and investigating crime, analysing and managing commercial risks
- i. project management
- j. providing media announcements and responses
- k. requesting feedback or participation in surveys, as well as conducting market research and/or analysis for statistical, profiling or other purposes for us to design our [products / services], understand customer behaviour, preferences and market trends, and to review, develop and improve the quality of our products and services
- l. managing the safety and security of our premises and services (including but not limited to carrying out CCTV surveillance and conducting security clearances)
- m. managing and preparing reports on incidents and accidents
- n. organising events, seminars or trainings
- o. complying with any applicable rules, laws and regulations, codes of practice or guidelines, obligations, requirements or arrangements for collecting, using and disclosing personal data that apply to the Company
- p. to assist in law enforcement and investigations by relevant authorities
- q. archival management (including but not limited to warehouse storage and retrievals)

9. Disclosure of Personal Data

The Company may disclose your personal data, locally or overseas, to:

- a. Departments within the Company for the above use and purposes
- b. Networks
- c. Contracting parties
- d. Referrers who have referred you to the Company
- e. Agents, contractors, vendors, installers, or third-party service providers who provide administrative or operational services to the Company, such as data intermediaries, courier services, telecommunications, information technology, payment, payroll, processing, training, market research, storage, archival, customer support investigation services or other services to the Company
- f. Agents, contractors, vendors or other third-party service providers in connection with marketing, products and services offered by the Company

- g. Analytics, search engine providers or third-party service providers that assist us in delivering our products, services, websites and platforms as well as improving and optimising the same
- h. Any business partner, investor, assignee or transferee (actual or prospective) to facilitate business asset transactions (which may extend to any merger, acquisition or any debt or asset sale) involving any of the Company
- i. Professional advisers such as auditors and lawyers
- j. Relevant government regulators, government ministries, exchange, statutory boards or authorities or law enforcement agencies who have jurisdiction over the Company or any Company or over any transaction entered into by you
- k. Any liquidator, receiver, administrator, judicial manager, trustees-in-bankruptcy, custodian or other similar official who has been so appointed, pursuant to bankruptcy, winding-up or insolvency proceedings instituted in Singapore or elsewhere, in respect of you or your assets
- l. Third parties who organise promotional or marketing events, seminars or trainings
- m. Any other party to whom you authorise us to disclose your personal data to.

The Company will take reasonable steps to protect your personal data against unauthorised disclosure by overseas entities or organizations, check for transfer limitation obligation – by ensuring the recipient country or at least the recipient organization has data protection laws and policies.

10. On-going Notifications

- a. If you have provided your Singapore telephone number(s) and have indicated that you consent to receiving marketing or promotional information via your Singapore telephone number(s), then from time to time, the Company may contact you using such Singapore telephone number(s) (including via voice calls, text, fax or other means) with information about our products and services (including discounts and special offers).
- b. In relation to particular products or services or in your interactions with us, we may also have specifically notified you of other or new purposes for which we collect, use or disclose your personal data. If so, we will collect, use and disclose your personal data for these additional purposes as well, unless we have specifically notified you otherwise.
- c. If you do not wish to receive any calls from us, please let us know and we shall act accordingly.
- d. We will try our best to comply with PDPA and upon being aware of a data breach, we will take prompt actions to attend to the breach and notify the relevant stakeholders timely. Any individuals, including our employees, representatives and clients, should notify us as soon as possible upon being aware of a data breach of personal data processed by us or suspect such breach.

11. Use of Cookies and Related Technologies

- a. The Company's websites and platforms use cookies and other technologies. Cookies are small text files stored in your computing or other electronic devices when you visit our website and platforms for record keeping purposes. Cookies are stored in your browser's file directory, and the next time you visit the website or platform, your browser will read the cookie and relay the information back to the website, platform or element that originally set the cookie. Depending on the type of cookie it is, cookies may store user preferences and other information.
- b. Web beacons (also known as pixel tags and clear GIFs) involve graphics that are not apparent to the user. Tracking links and/or similar technologies consist of a few lines of programming code and can be embedded in our websites or platforms. Web beacons are usually used in conjunction with cookies and primarily used for statistical analysis purposes. This technology can also be used for tracking traffic patterns on websites and platforms, as well as finding out if an e-mail has been received and opened and to see if there has been any response.
- c. The Company may employ cookies and other technologies as follows:
 - i. tracking information such as the number of visitors and their frequency of use, profiles of visitors and their preferred sites
 - ii. making our websites and platforms easier to use. For example, cookies may be used to help speed up your future interactions with our websites and platforms
 - iii. to better tailor our products and services to your interests and needs
 - iv. collating information on a user's search and browsing history
 - v. when you interact with us on our websites and platforms, we may automatically receive and record information on our server logs from your browser. We may collect for the purposes of analysis, statistical and site-related information including, without limitation, information relating to how a visitor arrived at the website or platform, the browser used by a visitor, the operating system a visitor is using, a visitor's IP address, and a visitor's click stream information and time stamp (which may include for example, information about which pages they have viewed, the time the pages were accessed, and the time spent per web page)
 - vi. using such information to understand how people use our websites and platforms, and to help us improve their structure and contents
 - vii. using cookies that are necessary in order to enable our websites and platforms to operate, for example, cookies that enable you to log onto secure parts of our websites and platforms
 - viii. personalising the website and platform for you, including delivering advertisements which may be of particular interest to you and using cookie related information to allow us to understand the effectiveness of our advertisements.

- d. Some cookies we use are from third party companies to provide us with web analytics and intelligence about our websites and platforms. These companies collect information about your interaction with our websites and platforms. We use such information to compile statistics about visitors who interact with the websites, platforms and other companies' online content, to gauge the effectiveness of our communications, and to provide more pertinent information to our visitors.
- e. If you do not agree to our use of cookies and other technologies as set out in this Data Protection Policy, you should delete or disable the cookies associated with our websites and platforms by changing the settings on your browser accordingly. However, you may not be able to enter certain part(s) of our websites or platforms. This may also impact your user experience while on our websites or platforms.
- f. Third-Party Sites: Our website may contain links to other websites operated by third parties. We are not responsible for the data protection policies or privacy practices of websites operated by third parties that are linked to our website. We recommend you learn about the policies and practices related to data of such third-party websites.

12. Data Protection Measures

This policy helps to protect the Company from data security risks.

- a. The Company keeps all physical data (non-electronic and electronic forms in data storage devices) confidential and under lock and key. Only authorised personnel are allowed access to that data required for providing the product or service. All personnel data are marked confidential.
- b. The Company will take reasonable efforts to protect personal data in our possession or our control by making reasonable security and IT arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Access of data is restricted to authorised personnel and to seniority of personnel. However, we cannot completely guarantee the security of any personal data we may have collected from or about you or prevent harmful code that enter our website. You should be aware of the risks associated with using websites and take necessary precautions.
- c. While all steps will be taken to protect your personal data, security of the information you transmit to us via the Internet or electronic communication or when you use our electronic services cannot be ensured. You should take every precaution to protect your personal data when you use such platforms. We recommend that you change your passwords often, use a combination of letters and numbers, and ensure that you use a secure browser.
- d. If applicable, you undertake to keep your username and password secure and confidential and shall not disclose or permit it to be disclosed to any unauthorised person, and to inform us as soon as reasonably practicable if you know or suspect that someone else knows your username and password or believe the confidentiality of your username and password has been lost, stolen or compromised in any way or that actual or possible unauthorised transactions have taken place. We are not liable for any damages resulting from any security breaches, on unauthorised and/or fraudulent use of your username and password.

13. Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is **stored on paper**, it will be marked “CONFIDENTIAL” and kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a **locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data to be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a USB device, external storage medium, CD or DVD), to be kept locked away securely when not being used.
- Data to only be stored on **designated drives and servers** and to be uploaded only to an **approved cloud computing services** which are PDPA compliant.
- Servers containing personal data to be **sited in a secure location**, away from general office space.
- Data to be **backed up frequently**. Those backups should be tested regularly, in line with the company’s standard backup procedures and where possible to be encrypted and password protected.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.
- CCTV footage will be housed in external HDDs that are encrypted and accessible only by password using Password Management Policy.

14. Data accuracy

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff will not create any unnecessary additional data sets.
- Staff will **take every opportunity to ensure data is updated** by follow up calls or emails and recording them.
- The Company will make it **easy for data subjects to update the information** the Company holds about them such as on company websites.
- Data to be **updated as inaccuracies are discovered**.

15. Access & Correction Requests

All individuals who are the subject of personal data held by the Company are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it but must specify the type of data and time range.
- Be informed **how to keep it up to date**.
- Be informed how the company is **meeting its data protection obligations**.
- Correct any **mistakes or update** their personal data in possession of the Company

Access

An individual can contact the Company and request for her/his personal data (Access Request) via the Personal Data Application Form (write in to our DPO to receive a copy of this form)

Access Requests from individuals should be made by email, addressed to the DPO. The DPO may supply a standard request form, although individuals do not have to use this.

Individuals may be charged a reasonable fee per Access Request to defray minimum costs. This may also increase depending upon the extent and effort of procuring the personal data. The DPO will aim to provide the relevant data within 30 calendar days.

For security reasons, the DPO will always verify the identity of anyone making an Access Request before handing over any information.

Correction

Correction requests will be carried out within 30 calendar days. No charge will be levied for any correction requests.

You have the right to request that we amend or update your personal data where it is inaccurate or incomplete. Kindly note that while we shall make a reasonable effort to ensure that the Personal Data we collect is accurate and complete, you are responsible for ensuring the accuracy of the Personal Data that you provide to us directly.

We will respond to your correction request as soon as reasonably possible. Should we not be able to perform the correction request within 30 days after receiving your request, we will inform you in writing via email on the time by which we will be able to perform your correction request. If we are unable to perform a correction requested by you, we shall generally inform you of the reasons why we are unable to do so (except where we are not required to do so under the PDPA or under any other applicable laws). If dissatisfied with the refusal to correct the personal data, individuals could email to DPO with other supporting documents to request for correction. DPO may assess the situation on case by case scenario.

Unsolicited Personal Data: In the event information is provided in hard copy or website without our specific collection of data, you agree that you hereby give your consent for our collection, use, and disclosure of this data to fulfil the purpose specified by you / respond to your query. Please let us know if you would like to withdraw your consent using our Personal Data Application Form.

16. Withdrawal of Consent

You have right to withdraw your consent at any time, where consent is the legal basis of the processing of your personal data. Kindly note that depending on the nature and scope of your request, we may not be in a position to continue performing our obligations in the course of or in connection with providing the service to you.

Upon reasonable notice being given by an individual, including client, representative, employee, job applicant and general inquirer, of his/her withdrawal of any consent given or deemed to have been given in respect of our collection, use or disclosure of his personal data, we will inform the individual of the likely consequences of withdrawing consent. We will cease collecting, using or disclosing the personal data unless it is required or authorised under applicable laws within 30 days.

You may also request us to erase or to stop processing of all or some of your personal data. We will process such instruction whenever possible except if we are not able to do so and we shall provide explanation to you.

17. Retention of Personal Data

So long as you have a direct or indirect relationship with the Company, your personal data will be held and processed in accordance with this Policy. Once the relationship ends or you withdraw all your personal data, the Company will not retain your personal data unless there are legal and / or business reasons for so doing.

Personal data will be retained by the Company till purpose is fulfilled. This is subject to sectoral and other written laws which includes law relating to the sector the Company does business in, employment laws, CPF, income tax laws, Limitation Act, and other regulations thereunder.

18. Transfers of Personal Data Outside Of Singapore

We generally do not transfer your personal data to countries outside of Singapore. However, if we do so, we will obtain your consent for the transfer to be made and we will take steps to ensure that your personal data continues to receive a standard of protection that is at least comparable to that provided under the PDPA.

19. Data Protection Officer

You may contact our Data Protection Officer if you have any enquiries, feedback, questions, or comments on our personal data protection policies and procedures, or if you wish to make any complaints or request, in the following manner:

Name of DPO : Siti Zuhra
Contact No. : +65 6343 4305
Email Address : enquiries@alnasry.sg
Address : 552 Hougang Street 51, #B1-296, Singapore 530552

20. Effect of Notice And Changes To Notice

This Notice applies in conjunction with any other notices, contractual clauses and consent clauses that apply in relation to the collection, use and disclosure of your personal data by us.

We may revise this Notice from time to time without any prior notice. You may determine if any such revision has taken place by referring to the date on which this Notice was last updated. Your continued use of our services constitutes your acknowledgement and acceptance of such changes.

21. Governing Law

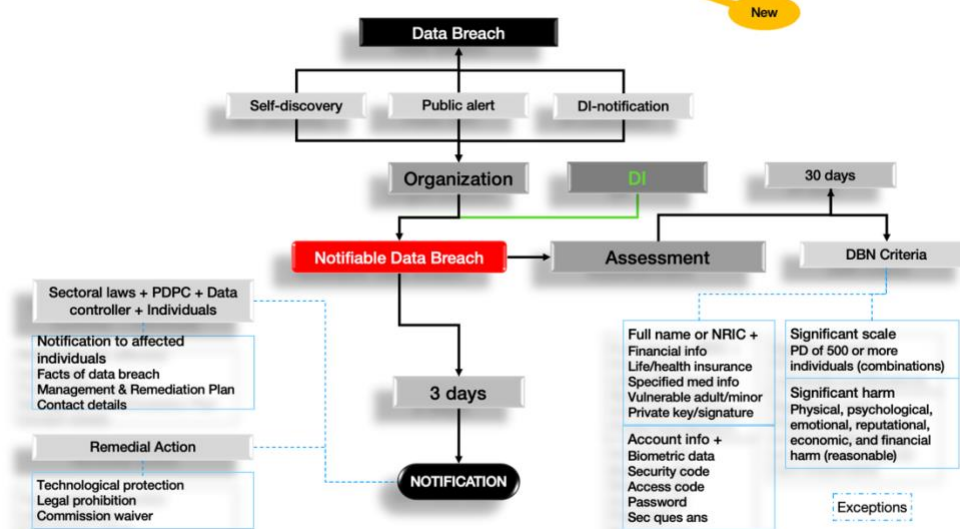
This Data Protection Policy shall be governed in all respects by the laws of Singapore.

22. Data Breach Management Plan

Should there be a breach of data, the Data Protection Officer (DPO) will activate the Data Breach Management Plan as detailed below:

Step	Action	Responsibility
A	<p>Report data breach incident to the DPO via email with the following details :</p> <ul style="list-style-type: none"> • Date and time of event • Name of the person who reported the case • A brief description of the nature of the data breach 	Anyone
B	<p>Data Breach Incident Form:</p> <p>Initiate meeting (through phone, email or face to face) with the person who reported the case to collect tangible evidence of the case :-</p> <ul style="list-style-type: none"> • Source of the data leakage – How did the person find out the case. • Nature of data leaked • Person(s) affected by the leak <p>DPO to record details of meeting in the <u>Data Breach Incident Form</u> and get the person who reported the case to sign on the form.</p>	DPO & Person Concerned
C	<p>Assessment Review:</p> <p>Facts gathered and assess the level of risk of the data breach and propose corrective action (CA) and/or preventive action (PA) measures and present to the Senior Management Committee for approval of action. Senior Management Committee will escalate to Board of Directors/Shareholders if deemed necessary.</p> <p>DPO to record the assessment in the Data Breach Incident Form. Update to DBMP activity log.</p>	DPO
D	<p>Notification:</p> <p>Upon approval by the Senior Management Committee, DPO to carry out the Corrective / Preventive Action and close the case.</p> <p>Notify relevant parties involved, Sectoral Laws, PDPC, Data Controller + Data Intermediaries + Individuals.</p>	DPO
E	<p>Post Evaluation Review:</p> <p>Explore root cause analysis and Post Breach action taken, the team will conduct review and Improve policy and procedures.</p>	DPO

Data Breach Notification



Flowchart created and designed by Yang Yen Thaw © Dec 2020

Timeframes for Managing Data Breach Process (within 30 days)

- 1) Data Incident suspected - Within 24 hours
- 2) Data Breach Confirmed - Without delay
- 3) Data Breach Notification- Within 30 days (PDPC, DI, Affected Individuals)
- 4) Responding to Data Breach
- 5) Corrective/Preventive Actions - With immediate effect