PRIVACY POLICY

Last updated: Dec 22, 2023

---

1. Overview

Customer personal data is important and it is our policy to respect the confidentiality of information and the privacy of individuals. This Policy articulates how TokenPay Pte Ltd. manages and protects customer data we hold in compliance with the Personal Data Protection Act in Singapore (the “Act”). We will also comply with local data protection and privacy laws in our operations out of Singapore, as and when required.

2. Personal data

As used in this Notice: “customer” means an individual who:

(a) has contacted us through any means to find out more about any goods or services we provide, or

(b) may, or has, entered into a contract with us for the supply of any goods or services by us; and “personal data” means data, whether true or not, about a customer who can be identified:

(i) from that data; or

(ii) from that data and other information to which we have or are likely to have access. Depending on the nature of customer interaction with us, some examples of personal data which we may collect include name and identification information such as NRIC or Passport number, contact information such as address, email address or telephone number, nationality, date of birth, and other audio-visual information, employment information and bank account information. Other terms used in this Notice shall have the meanings given to them in the the Act, where the context so permits.

2.1 What types of personal data do we collect?

We may collect and hold personal data of persons/entities including but not limited to:

- Customers;
- Job applicants and employees;
- Shareholders;
- Service providers; vendors, business partners, and
- Other people who we may come into contact with

Examples of such personal data include curriculum vitae, contact details, account information and your preferences, queries, requests and feedback.

2.2 How do we collect customer personal data?
The ways in which we may collect personal data include (but are not limited to) collecting directly or indirectly from you or your authorized representatives in the course of:

- signing up for alerts
- visiting our website;
- applying for a job or internship;
- participating in Company marketing or promotional events;
- using the company's products or services;
- contacting us with queries, requests, complaints, or feedback;
- conducting or completing of transactions;
- conducting market research or customer engagement or other surveys;
- conducting interviews

2.3 What kind of purposes do we collect customer personal data for?

In general, we may use your personal data for the following purposes:

- conducting and completing transactions (e.g. processing transactions and payments; providing products or services that have been requested);
- providing customer service (e.g. responding to queries and requests; informing the customer about queries and product updates; and sending you alerts);
- conducting market research and improving customer service (e.g. conducting market research or surveys; performing market analysis; managing and enhancing Company products and services; developing new products);
- conducting marketing promotions (e.g. sending of alerts, marketing materials and invitations from us wholly or through affiliation with third parties; offering promotions and loyalty programs);
- complying with applicable laws, regulations and other requirements (e.g. providing assistance to law enforcement agencies, regulatory authorities and other governmental agencies;performing internal audits);
- maintaining investor relations (e.g. sending of alerts, marketing materials and invitations from us wholly or through affiliation with third parties);
- performing evaluations (e.g. assessing suitability of employees).

2.4 When do we collect customer NRIC or other national identification numbers?

We will not collect NRIC or other national identification numbers (such as Birth Certificate numbers, Foreign Identification Numbers (FIN), Work Permit numbers and passport numbers), or copies of such documents, unless required by law or where it is necessary to accurately establish or verify the customer's identity to a high degree of fidelity, to comply with relevant regulatory requirements.

2.5 How do we use and/or disclose customer personal data?

We will only use, disclose and/or transfer customer personal data for the purposes that the customer has been notified of and consented to or which are permitted under applicable laws and regulations.

The Group will not sell, or give away personal data to third parties for commercial purposes without customer consent.

2.6 Who do we share customer personal data with?

Depending on the product or service concerned, personal data may be disclosed or transferred to:

- other divisions or organizations within the Group;
- joint venture/ alliance partners or other investors;
- service providers and specialist advisers/institutions who have been contracted to provide administrative, financial, legal, accounting, information technology, research or other services;
- insurers, credit providers, courts, tribunals, law enforcement agencies, regulatory authorities and other governmental agencies as agreed or authorized by law;
- credit reporting or reference agencies or insurance investigators;
- anyone authorized by the customer, as specified by the customer during any contract with the customer.

Where personal data is disclosed or transferred to organizations outside of the Group who handle or obtain personal data as service providers to the Group, we require such organizations to acknowledge the confidentiality of such personal data, undertake to respect any individual's right to privacy and comply with the Act and this Policy and use such personal data only for our purposes and otherwise follow our reasonable directions with respect to this data.

2.7 Collection of sensitive data

The Group does not collect sensitive information without the individual's consent and unless it is specifically relevant and necessary for it's primary purposes of conducting, improving, maintaining and developing a business relationship.

2.8 How do we manage, protect and store your personal data?

The GroupCompliance department is responsible to oversee our management of personal data in accordance with the Act. We regard breaches of your privacy very seriously and we have implemented measures to secure and protect your information, such as training our employees who handle your personal data to respect the confidentiality of such personal data and your privacy, storing personal data in a combination of secure computer storage facilities and paper based files and other records, taking steps to protect the personal data we hold from misuse, loss, unauthorised access, modification or disclosure.

However, you will appreciate that it is not for us to perfectly secure your personal data from cyber attacks, such as hacking, spyware and viruses. Accordingly, you will not hold us liable for any unauthorized disclosure, loss or destruction of your personal data arising from such risks. The Act also requires us not to store personal data longer than is required by the data retention policy. We will cease to retain your personal data when we no longer require such personal data for the purposes we originally notified you of or for any business or legal needs.

2.9 How do we keep personal data accurate and up-to-date and how to exercise your right to correct the personal data we hold of you?

The Group Compliance department is responsible to oversee our management of personal data in accordance with the Act. We endeavour to ensure that the personal data we hold about you is accurate and up-to-date, and stored securely. We realize that such personal data changes frequently with changes of address and other personal circumstances. We encourage you to contact us as soon as possible in order to update any personal data we hold about you. Please complete the Personal Data Correction Form and send us your updated details. Our contact details are set out below. We may require you to verify your identity in such instances.
However, you will appreciate that it is not for us to perfectly secure your personal data from cyber attacks, such as hacking, spyware and viruses. Accordingly, you will not hold us liable for any unauthorized disclosure, loss or destruction of your personal data arising from such risks. The Act also requires us not to store personal data longer than is required by the data retention policy. We will cease to retain your personal data when we no longer require such personal data for the purposes we originally notified you of or for any business or legal needs.

2.10 How to exercise your right to access the personal data we hold of you?

You have the right to:

- Access your personal information
- Correct your personal information
- Delete your personal information
- Object to the processing of your personal information

- Withdraw your consent to the processing of your personal information
- Lodge a complaint with a supervisory authority

Please contact us if you wish to exercise any of these rights.

To make a request to access the personal data we hold about you, you may contact the The Group compliance department in writing using the Request to Access Personal Data Form. We will require you to verify your identity and to specify what data you require. We may charge a fee to cover the cost of verifying the application and locating, retrieving, reviewing and copying any material requested. If the data sought is extensive, we will advise the likely cost in advance and can help to refine your request if required.

2.11 How do we manage personal data stored on blockchains using Distributed Ledger Technologies?

The Group will employ off-chain approaches that store customer personal data in centralised databases / repositories, which will be encrypted and have the necessary access controls in place, while only writing representations of the personal data onto the block chain. Only a hash of the personal data or a hash of the link to the off-chain database would be written on-chain. Hashes are cryptographically generated strings that serve as irreversible, 1-1 representations of the hashed data. Any change in the underlying data will generate a completely different hash. This allows the hash to be used as a digital signature that, if written on-chain, will serve as an immutable verification of the underlying data's integrity.

2.12 How do you make a complaint regarding misuse of personal data?

If you consider that any action of the Group breaches the Act or this Policy, you can make a complaint to the Group Compliance department by completing the Complaint Form. We will endeavour to act promptly in response to a complaint.

3. Collection, use and disclosure of personal data

We generally do not collect your personal data unless:

(a) it is provided to us voluntarily by you directly or via a third party who has been duly authorised by you to disclose your personal data to us (your "authorised representative") after (i) you (or your authorised representative) have been notified of the purposes for which the data is collected, and (ii) you (or your authorised representative) have provided written consent to the collection and usage of your personal data for those purposes, or

(b) collection and use of personal data without consent is permitted or required by the the Act or other laws.We shall seek your consent before collecting any additional personal data and before using your personal data for a purpose which has not been notified to you (except where permitted or authorised by law).

We may collect and use your personal data for any or all of the following purposes:
(a) performing obligations in the course of or in connection with our provision of the goods and/or services requested by you;
(b) verifying your identity;
(c) responding to, handling, and processing queries, requests, applications, complaints, and feedback from you; managing your relationship with us; processing payment or credit transactions; sending your marketing information about our goods or services including notifying you of our marketing events, initiatives and promotions, lucky draws, membership and rewards schemes and other promotions; complying with any applicable laws, regulations, codes of practice, guidelines, or rules, or to assist in law enforcement and investigations conducted by any governmental and/or regulatory authority; any other purposes for which you have provided the information; transmitting to any unaffiliated third parties including our third party service providers and agents, and relevant governmental and/or regulatory authorities, whether in Singapore or abroad, for the aforementioned purposes; and any other incidental business purposes related to or in connection with the above.

We may disclose your personal data where such disclosure is required for performing obligations in the course of or in connection with our provision of the goods or services requested by you; or to third party service providers, agents and other organisations we have engaged to perform any of the functions listed above for us.The purposes listed in the above clauses may continue to apply even in situations where your relationship with us (for example, pursuant to a contract) has been terminated or altered in any way, for a reasonable period thereafter (including, where applicable, a period to enable us to enforce our rights under any contract with you).

4. HOW WE USE COOKIES

We do not collect or use cookies for any purposes. However, as we use Google as a service provider to manage our website, they offer several products, including AdSense, Google Ads, Google Analytics, and a range of products within the Google Marketing Platform. When users visit a page or see an ad that uses one of these products, either on Google services or on other sites and apps, various cookies may be sent directly to the Google browser.

These may be set from a few different domains, including google.com, doubleclick.net, googlesyndication.com, and googleadservices.com. Some of their advertising and measurement products enable services like Google Analytics, and these services may send their own cookies to your browser. Please note that these cookies will be set from their domains directly.

4.1 MANAGING COOKIES:

You can control the use of cookies through your browser settings. Most browsers allow you to block cookies, delete cookies, or set preferences for certain websites.Please note that if you disable cookies, some features of our website may not work properly.

5. Withdrawing customer consent

The consent that you provide for the collection, use and disclosure of your personal data will remain valid until such time it is being withdrawn by you in writing. You may withdraw consent and request us to stop using and/or disclosing your personal data for any or all of the purposes listed above by submitting your request in writing or via email to our Compliance department at the contact details provided below. Upon receipt of your written request to withdraw your consent, we may require reasonable time (depending on the complexity of the request and its impact on our relationship with you) for your request to be processed and for us to notify you of the consequences of us acceding to the same, including any legal consequences which may affect your rights and liabilities to us. In general, we shall seek to process your request within ten (10) business days of receiving it. Whilst we respect your decision to withdraw your consent, please note that depending on the nature and scope of your request, we may not be in a position to continue providing our goods or services to you and we shall, in such circumstances, notify you before completing the processing of your request. Should you decide to cancel your withdrawal of consent, please inform us in writing in the manner described in clause 8 above. Please note that withdrawing consent does not affect our right to continue to collect, use and disclose personal data where such collection, use and disclose without consent is permitted or required under applicable laws.

6. Access to and correction of personal data

If you wish to make
(a) an access request for access to a copy of the personal data which we hold about you or information about the ways in which we use or disclose your personal data, or
(b) a correction request to correct or update any of your personal data which we hold about you, you may submit your request in writing or via email to our Compliance department at the contact details provided below.

Please note that a reasonable fee may be charged for an access request. If so, we will inform you of the fee before processing your request. We will respond to your request as soon as reasonably possible. Should we not be able to respond to your request within thirty (30) days after receiving your request, we will inform you in writing within thirty (30) days of the time by which we will be able to respond to your request. If we are unable to provide you with any personal data or to make 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 the Act).

7. Protection of personal data

To safeguard your personal data from unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks, we have introduced appropriate administrative, physical and technical measures such as up-to-date antivirus protection, encryption and the use of privacy filters to secure all storage and transmission of personal data by us, and disclosing personal data both internally and to our authorised third party service providers and agents only on a need-to-know basis. You should be aware, however, that no method of transmission over the Internet or method of electronic storage is completely secure. While security cannot be guaranteed, we strive to protect the security of your information and are constantly reviewing and enhancing our information security measures.

8. Accuracy of personal data

We generally rely on personal data provided by you (or your authorised representative). In order to ensure that your personal data is current, complete and accurate, please update us if there are changes to your personal data by informing our Compliance department in writing or via email at the contact details provided below.

9. Retention of personal data

We will cease to retain your personal data, or remove the means by which the data can be associated with you, as soon as it is reasonable to assume that such retention no longer serves the purpose for which the personal data was collected, and is no longer necessary for legal or business purposes.

As a general policy requirement, both customer personal data and customer transaction data will be held for a minimum period of 5 years, after account closure or termination of relationship.

10. 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.

11. Transfers of personal data outside 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 the Act.

12. Updates to this policy

This Policy will be reviewed from time to time to take account of new laws and technology, changes to our operations and practices and the changing business environment.

13. Third party privacy policies may apply

Our website may contain links to websites operated by third parties. If you visit such third party websites, this Personal Data Protection Policy may not apply.

14. How to contact us?

For any enquiry or request regarding this privacy policy, you can contact our compliance department by email: sohrab.setna@rivo.network.