

Privacy Policy

Scope and Consent

We want you to understand why and how Triple A Technologies Pte Ltd and its subsidiaries, affiliates, associated companies, and jointly controlled entities, including Paytop SAS (Triple-A Europe), Triple A Technologies Inc. (Triple-A US), Triple A Technologies Limited (Triple-A Hong Kong) and Triple A Technologies FZCO (Triple-A UAE) ("**Triple-A**", "we", "us" and/or "our") collects, uses, discloses and or/processes your Personal Data (as defined below) including but not limited to Singapore's Personal Data Protection Act 2012 ("PDPA"), the European Union General Data Protection Regulation ("EU GDPR"), the relevant United States privacy laws, such as the California Consumer Privacy Act ("CCPA"), where applicable, the Hong Kong Personal Data (Privacy) Ordinance ("PDPO"), and the United Arab Emirates Federal Decree Law No. (45) of 2021 on the Protection of Personal Data ("UAE PDPL") and its implementing regulations.

This Privacy Policy ("**Policy**") applies to you and all Individuals (as defined below) who provide Triple-A with Personal Data or whose Personal Data is otherwise collected, used, processed, stored and/or disclosed by Triple-A in connection with and/or for the purposes of its operations.

This Policy supplements but does not supersede or replace any previous consent which you may have provided to Triple-A, nor does it affect any legal rights that Triple-A may have regarding the collection, use, processing and/or disclosure of any Individual's Personal Data.

Triple-A may from time to time update this Policy to ensure that it is consistent with our business needs or to accommodate amendments to applicable legal or regulatory requirements. All updates to this Policy will be published online at www.triple-a.io (the "**Triple-A Website**").

Notification of any material revisions will also be published on the Triple-A Website. You shall be deemed to have accepted the Policy as amended by continuing your relationship with Triple-A after any amendments have been published on the Triple-A Website.

This Policy forms part of the terms and conditions, if any, governing your specific relationship with Triple-A ("**Terms and Conditions**") and it should be read in conjunction with the 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 to the fullest extent permissible by law.

1. Definitions

For the purposes of this Policy:

- "**Individual**" (or "**you**") means a natural person, whether living or deceased and "**Individuals**" (and "**your**") shall be construed accordingly;
- "**Personal Data**" means data that is capable of identifying an Individual, whether on its own or in conjunction with other data accessible to Triple-A;
- "**Personnel** " means any Individual engaged under a contract of service with Triple-A including permanent or temporary employees as well as trainees and interns engaged by Triple-A from time to time; and
- "**Potential Personnel**" means any Individual who has submitted an application to be engaged by Triple-A as Personnel.

2. Purposes for collection, use and disclosure of Personal Data

Triple-A will only collect, use and disclose Personal Data from/or related to an Individual that is reasonably considered necessary for the relevant purposes underlying such collection, use or disclosure, which may include but is not limited to the following:

- Provide our Services (including customer support);
- Process transactions and send notices about your transactions;
- Resolve disputes, collect fees, and troubleshoot problems;
- Communicate with you about our Services and business and to inform you of matters that are important for your account and/or use of the Sites. We also use your personal data to respond to any questions, comments or requests you filed with us and the handling of any complaints;
- Comply with applicable laws and regulations;
- Establish, exercise and defend legal claims;
- Monitor and report compliance issues;
- Customise, measure, and improve our business, the Services, and the content and layout of our website and applications (including developing new products and services; managing our communications; determining the effectiveness of our sales, marketing and advertising; analysing and enhancing our products, services, websites and apps; ensuring the security of our networks and information systems; performing accounting, auditing, invoicing, reconciliation and collection activities; and improving and maintaining the quality of our customer services);
- Perform data analysis;

- Deliver targeted marketing, service update notices, and promotional offers based on your communication preferences, and measure the effectiveness of it. To approach you via email for marketing purposes, we request your consent, unless it is not required by law. You always have the option to unsubscribe from our mailings, e.g., via the unsubscribe link in our newsletter;
- Perform risk management, including comparing information for accuracy and verify it with third parties and protect against, identify and prevent fraud and other prohibited or illegal activity, claims and other liabilities; and
- Enforce our contractual terms.

3. What Information that we may collect?

The exact Personal Information which we may collect from you will differ depending on if you are visiting a Triple-A website/social media account, or if you are onboarded or in the process of being onboarded for the use of our Services. Some of the Personal Data which we may collect through your interaction with us, depending on the mode of interaction, may include your/the:

- First and last name;
- Country and city of residence;
- Location data;
- Job title;
- Nationality of legal representatives and senior management members;
- % shares/voting rights in the company;

- Phone number;
- ID number;
- Date of birth;
- Date of birth and nationality of individuals owning or controlling directly and indirectly more than 10% in the company;
- First and last name and/or billing first and last name and/or shipping name
- Billing address (street, city, state, country, zip code) and/or shipping address
- Email and/or billing email and/or shipping email
- Phone and/or billing phone number and/or shipping phone number
- Billing company and/or shipping company
- Username
- User ID
- Shopping cart items information : for each item, the SKY, price, quantity and name of the item
- Shopping cart checkout information: shipping cost, tax cost, shipping discount
- Any online identifier; and
- Any factors that may be used to identify you.

This is not an exhaustive list. Depending on how you interact with us, we may collect additional information, as required.

In case Personal Data that you provide to us or we collect is considered special categories of Personal Data or judicial data under applicable data protection laws, we only process them to the extent permitted by applicable law. Special categories of Personal Data may include Personal Data from which we can determine or infer an individual's racial or ethnic origin, political opinions, religious or, trade union membership, genetic data, data concerning health, sexual life or sexual orientation. Judicial data may include data relating to criminal convictions and offences, including information concerning the commission or alleged commission of a criminal offence

Personal Data does not include data where any potential identifiers have been irreversibly removed (anonymous data).

4. How we collect Personal Data

Generally, Triple-A may collect Personal Data from you in one or more of the following ways or circumstances:

- Information provided directly: You may be asked to provide Personal Data when you visit or use some parts of our websites and/or services. You do not have to provide us with your Personal Data; however, it could mean that you are not able to access some parts of our website or use our services.
- Information collected automatically: Some information is collected automatically, such as an IP address and device type, when you visit our websites or use our services. This information is useful to us as it provides us with a better understanding of how you are interacting with our websites and services so that we can continue to provide you with the best experience possible.

- Information from third parties: The majority of information that we collect is collected directly from you. Some data may be collected from other sources, such as information that is available in the public domain. We use this information to supplement the Personal Data that we have collected from you.

5. How we use Personal Data and Other Information

We may use personal and other information for our legitimate business interests, to the extent permitted by applicable law, including but not limited to:

- Complete your transactions, respond to your questions, and provide you with customer service;
- Send you transactional and other administrative messages;
- Personalise your experience when you use our services;
- Operate and grow our business (e.g., conduct data analysis; audit our activities; develop new products; enhance, improve and modify our services; identify usage trends; determine the effectiveness of our promotional campaigns);
- Monitor and prevent fraud, money laundering, abuse, and other actual and potential prohibited or illegal activities;
- Meet legal, auditing, regulatory, insurance, security and processing requirements;
- Report to credit bureaus;
- Respond to court orders and legal investigations;

- Deliver marketing communications to you about our services and other companies' services, including offers, coupons or incentives we believe may be of interest to you;
- Comply with applicable laws, which may include laws outside your country of residence;
- Respond to requests from public and government authorities, which may include authorities outside your country of residence;
- Cooperate with law enforcement, or for other legal reasons
- Enforce our terms and conditions; and
- Protect our rights, privacy, safety or property, and/or that of our affiliates, you or others. We may also use information in other ways with your consent or as required by applicable law.

In the event of a data breach, Triple-A will notify the relevant supervisory authority and affected individuals as required by applicable data protection laws.

6. How we protect your data

Triple-A shall make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks to Personal Data in its possession.

If Triple-A transfers Personal Data outside of Singapore, the European Union, the United States Hong Kong, or the United Arab Emirates, it will take reasonable steps to ensure that such data receives a level of protection comparable to that provided under the Personal Data Protection Act 2012 (PDPA), the EU General Data Protection Regulation (GDPR), the relevant U.S. state and federal privacy laws, such as the California Consumer Privacy Act (CCPA), the Hong Kong

Personal Data (Privacy) Ordinance (PDPO), and the UAE Federal Decree Law No. 45 of 2021 on the Protection of Personal Data (UAE PDPL).

Such transfers shall be subject to this Policy, and Triple-A will implement appropriate technical, organisational, and contractual safeguards, including but not limited to standard contractual clauses, data processing agreements, and binding corporate rules where applicable, to ensure compliance with the data protection requirements of each jurisdiction.

Triple-A will ensure that third parties who receive Personal Data from Triple-A protect such Personal Data in a manner consistent with this Policy and not use such Personal Data for any purposes other than those specified by Triple-A, by incorporating appropriate contractual terms in its written agreements with third parties.

Triple-A is not responsible in any way for the security and/or management of Personal Data shared by you with third party websites accessible via links on Triple-A's website.

Please know, however, that no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure, please contact us immediately.

7. How we share data with third parties

We share and disclose information with:

- **Internal departments** – To fulfill the purposes described in this policy, your Personal Data may be shared with our internal teams (such as compliance, risk, and support) on a need-to-know basis or where there is

a legitimate interest, in line with applicable legal bases under each jurisdiction's data protection laws.

- **Authorised service providers** – We engage third-party vendors for IT services, website hosting, analytics, infrastructure, payment processing, order fulfillment, customer service, and email delivery. These vendors are contractually required to handle your Personal Data securely and in accordance with applicable data protection obligations.
- **Marketing and communications providers** – Where permitted under law or with your explicit consent, we may share your information with marketing service providers to manage communications and campaigns. Your choices and opt-out rights are respected under each applicable law (e.g., GDPR consent, CCPA opt-out, PDPO usage limitation).
- **Social media platforms and other users** – When you interact with our platforms or authorize sharing, your information may be disclosed to your social media connections or account providers, subject to your settings and applicable laws.
- **Corporate transactions** – In the event of a merger, acquisition, restructuring, or sale of our business or assets (including bankruptcy), we may transfer your Personal Data as part of the transaction, ensuring the receiving party complies with applicable privacy laws.
- **Legal obligations and rights protection** – We may disclose Personal Data where required by law, regulation, court order, or governmental request. This includes cooperation with relevant authorities in Singapore (e.g., PDPC), the EU (e.g., data protection authorities), Hong Kong (e.g., PCPD), the United States (e.g., state or federal regulators), and the UAE (e.g., UAE Data Office or VARA).

- **Retention requirements** – We may retain your personal data for as long as it is necessary to fulfil the purpose for which it was collected, or as required or permitted by applicable laws in jurisdictions like Singapore, the EU, Hong Kong, the U.S. and the UAE. This includes considerations such as when the information was collected or created, whether we are required to hold the information to comply with our legal obligations, including compliance or other financial regulatory obligations, or information preservation requirements.
- **Jurisdiction-specific disclosures:**
 - Singapore: We share personal data only with parties who meet the consent or deemed consent requirements under the Personal Data Protection Act (PDPA). Cross-border transfers of personal data are carried out in accordance with the PDPA's data transfer rules, including ensuring a comparable standard of protection.
 - European Union: All data sharing is subject to a lawful basis under the General Data Protection Regulation (GDPR) (e.g., contract performance, legitimate interest, or consent). Transfers of personal data outside the EU/EEA are conducted using appropriate safeguards, such as Standard Contractual Clauses (SCCs) or other approved mechanisms.
 - Hong Kong: We comply with the Personal Data (Privacy) Ordinance (PDPO), adhering to Data Protection Principles such as data accuracy, purpose limitation, and use restriction. Personal data is shared only where it is necessary, lawful, and proportionate.
 - United States: We comply with applicable federal and state privacy laws, including the California Consumer Privacy Act (CCPA) and its amendment, the California Privacy Rights Act (CPRA). We provide mechanisms for

individuals to exercise their rights to access, delete, or opt out of the sale or sharing of personal data, where applicable.

- United Arab Emirates (UAE): We comply with the UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (PDPL) and relevant sectoral regulations (such as those by the UAE Central Bank or VARA, where applicable). Personal data is processed lawfully, transparently, and for a specified purpose. Cross-border transfers are carried out in compliance with the PDPL's adequacy and safeguard requirements.

8. Request to Withdraw Consent

You have the right to withdraw your consent to the collection, use and/or disclosure of your Personal Data in the possession of Triple-A by submitting your request to Triple-A's Data Protection Officer at dpo@triple-a.io at any time.

We will process your request for the withdrawal of consent within a reasonable period of time from such a request being made. After that time, we will not collect, use and/or disclose your Personal Data in the manner stated in your request.

Your withdrawal of consent could affect the services that we are able to provide to you. Depending on the extent of your withdrawal of consent for us to process your Personal Data, it may mean that we are not able to continue with our existing business relationship.

With regards to data that is collected by cookies, you can manage your cookie preferences through our cookie banner/settings on Triple-A's Website. However, disabling the use of certain cookies may result in the loss of functionality, restrict your use of the website and/or delay or affect the way in which Triple-A's website operates.

9. Accuracy of Personal Data

Information voluntarily provided by you to Triple-A shall be deemed complete and accurate.

Triple-A will take reasonable steps to verify the accuracy of Personal Data received at the point of collection, but you will remain primarily responsible and liable to ensure that all Personal Data submitted by you to Triple-A is complete and accurate.

Triple-A will also take reasonable steps to periodically verify the Personal Data in its possession, taking into account the scope of its operations. However, you remain responsible for notifying Triple-A, from time to time, of any applicable changes to your Personal Data. You may notify the support team of any changes to your Personal Data by email at support@triple-a.io, or you may contact the Personal Data Officer by email at dpo@triple-a.io at any time.

Triple-A shall not be held liable for any inability on its part to provide services to you if you fail to ensure that your Personal Data submitted to Triple-A is complete and accurate.

10. Access to and correction of Personal Data

You may request:

- access to any Personal Data that is currently in our possession or control; and/or
- correction of any data that is currently in our possession or control by contacting us by email at dpo@triple-a.io.

For your protection, we may need to verify your identity before implementing your request.

When you request access to your Personal Data within our possession or control, we will seek to provide you with the relevant information within 10 business days.

Upon your written request, we will correct any inaccurate Personal Data that is within our possession or control within 10 business days.

With your consent, once we have corrected your Personal Data, we will send the corrected Personal Data to all organisations to which your Personal Data was disclosed by Triple-A within a year before the correction was made, unless that organisation does not require the corrected Personal Data for any legal or business purpose.

Triple-A is not required, under the PDPA, to provide access and correction to Personal Data in certain exempted situations as set out in the PDPA.

11. Retention of Data

The length of time we retain your personal data depends on its nature and whether we have a continuing business or legal need to do so.

We will retain your personal data for as long as we maintain a business relationship with you, and for a period thereafter where it is necessary to comply with our legal, regulatory, or operational obligations.

Once the relevant retention period has expired, and where there is no further business or legal need to retain your data, we will ensure it is securely deleted or anonymised.

Your personal data, including payment-related information, may be stored and maintained in jurisdictions such as Singapore, France, the United States, Hong Kong, or the UAE, depending on operational requirements and applicable regulatory frameworks.

Certain identity-related data and sensitive personal information (such as data considered “special categories of data” under the GDPR) may be retained beyond the standard retention period in accordance with applicable anti-money laundering (AML) laws and statutory data retention obligations in the relevant jurisdictions.

12. Making a complaint

You are welcome to contact us if you have any complaint or grievance about how we are handling any Personal Data in our control or possession.

To make a complaint you can:

- Contact our Data Protection Officer via email at dpo@triple-a.io.