Personal Information Collection Statement for RD Wallet

This notice, including its appendix/appendices, (the "**Notice**") should be read together with our Privacy Policy Statement, which sets out the privacy policies and practices applicable to our group companies including RD Wallet Technologies Limited and its successors and assigns (collectively, "**RD Technologies**" and "**we**", "**our**" or "**us**" shall be construed accordingly) in relation to the personal data we handle.

1 Collection of Data

(a) We may collect the personal data of individuals ("**you**" or "**your**") in connection with the provision of RD Wallet Services (as defined below) through our network-based stored value facility ("**RD Wallet**") and for the purposes set out in this Notice. "**RD Wallet Services**" means both new and existing services, facilities, products, website(s), mobile application(s), activities, marketing events and other events hosted, provided or made available by us relating to RD Wallet from time to time.

(b) You may be users of our RD Wallet Services, our business customers, individuals relating to our business customers, or business applicants applying for our RD Wallet Services (each a "**Business**")), including but not limited to:

(i) the sole proprietor, managers, employees, agents and officers of a sole proprietorship;

(ii) the shareholders, beneficial owners, directors, managers, employees, agents and officers of a corporation;

(iii) in the case where such person linked to a Business that is a trust, the trustees, settlors, protectors and beneficiaries of the trust;

(iv) in the case where such person linked to a Business that is a partnership, the partners of the partnership and members; and

(v) other persons who are related to the above Businesses or relevant to their relationship with us.

In this Notice, a "**relevant entity**" refers to each Business customer or Business applicant to which you are linked or related.

(c) In this Notice, "**personal data**" means any data (i) relating directly or indirectly to a living individual (which includes sensitive data such as biometric data, IP addresses and real time location), (ii) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (iii) in a form in which access to or processing of the data is practicable.

(d) We may collect and process some or all of the following personal data about you:-

(i) *your personal information*: this includes personal information that you provide to us when you use our RD Wallet Services, such as your name, biometric data, age, date of birth, identity card number, nationality, passport number;

(ii) *your contact information*: this includes telephone numbers, addresses, mailing addresses, WhatsApp, WeChat and other instant messaging account information, email addresses and fax numbers;

(iii) *your business information*: this includes your business name, business title, and your business contact information;

(iv) *your payment and account details*: this includes information on your (i) account(s) with us, (ii) transactions made using our RD Wallet Services, and (iii) bank accounts, and

credit, debit or other charge cards and other means of payment (including but not limited to your WeChat Wallet, Alipay account, Apple Pay), such as name of accountholder/cardholder, account/card number, billing address, security code and expiry date;

(v) *your photographs and videos*: this includes your facial images and videos being collected for customer due diligence purposes;

(vi) *your interest and preferences*: this includes your interests, personal preferences, comments and habits;

(vii) *survey and marketing information*: this includes your comments and responses to market surveys, contests and promotional offers conducted by us, in conjunction with us or on our behalf; and

(viii) *technical information*: this includes details of (i) your device particulars (including IMSI, IMEI, SEID and other phone numbers and information), and (ii) your visits to our websites, mobile application or social media platforms collected through cookies or other tracking technologies such as online behavioural information, browser details, IP addresses and location information.

(e) Your personal data is required for access to and use of our RD Wallet Services. If the personal data requested by us is not provided, we may be unable to provide (or continue to provide) our RD Wallet Services to you or the relevant entity(ies), or, even if we continue to provide you with certain level of access to our Services, the experience or quality may not be optimal.

(f) Your personal data may be:

(i) collected from you directly, from the relevant entity(ies), from someone acting on your behalf or from another source;

(ii) linked to or combined with data relating to entity(ies), if your data is linked to an entity(ies); and

(iii) combined with other data available to members of the "**Group**", meaning us and all of our holding companies, subsidiaries, joint ventures and associated entities, and a "**member**" of the Group shall be construed accordingly.

2 Use of Personal Data

(a) We may use personal data for one or more of the following purposes (which may vary depending on the nature of your relationship with us):

(i) processing applications for, and the daily operation of, our RD Wallet Services;

(ii) identifying and verifying the information of, and conducting client due diligence, anti-money laundering, fraud detection and transaction monitoring procedures on, you and/or the relevant entity(ies);

(iii) creating and maintaining our risk related models;

(iv) designing, maintaining, supporting and enhancing our RD Wallet Services, whether for your use or the use of the relevant entity(ies);

(v) conducting analysis, research and profiling to better understand your and the relevant entity's needs, preferences, interests, experiences and habits;

(vi) detecting, preventing and investigating crime and safeguarding public interest, which includes, where applicable, carrying out a matching procedure (as defined under the Personal Data (Privacy) Ordinance) by us;

(vii) exercising, enforcing and defending our rights and those of the Group, whether contractual, tortious or otherwise;

(viii) satisfying any operational, administrative and risk management requirements of our third party service providers;

(ix) meeting our obligations, requirements or arrangements or those of any member of the Group, whether compulsory or voluntary, to comply with or in connection with any applicable law or regulation, judgment, court order, sanctions regime, demand or request from any legal, regulatory, governmental or other authorities;

(x) complying with any obligations, requirements, policies, procedures, measures or arrangements for sharing personal data and information within the Group;

(xi) enabling actual or proposed assignee(s) of all or any part of our business and/or assets, or participant(s) or sub-participant(s) of our rights in respect of you to evaluate the transaction intended to be the subject of the assignment, participation or sub-participation and enabling the actual assignee(s) to use your personal data in the operation of the business or rights assigned;

(xii) communicating with you and/or the relevant entity(ies); and

(xiii) any other purposes relating or incidental to the purposes listed above.

3 Disclosure of Personal Data

(a) Personal data held by us will be kept confidential but we may provide personal data (whether in identifiable, unaggregated, aggregated, verified, unverified or anonymised form) to the following parties or any of them for the purposes set out in paragraph 2(a) above (the "**Transferee(s)**"):

(i) any member of the Group which has undertaken to keep such personal data confidential;

(ii) any counterparties, agents, contractors, sub-contractors or associates of us or the Group (as well as their respective, employees, officers, agents, contractors, service providers and professional advisers);

(iii) any third party service providers who provide administrative, marketing, customer due diligence, anti-money laundering, sanction compliance, name screening, fraud prevention, risks management, security, cryptography, distribution, data processing, communications, computer, payment , virtual account or other services to us or any member of the Group, including any person taking over or may take over all or part of our rights or obligations under the terms governing the aforesaid services or such person where such terms (or any part of it) is transferred to or may be transferred to;

(iv) any financial institution for the purposes of anti-money laundering related checks, fraud prevention and detection of crime;

(v) any local or foreign legal, regulatory, judicial, administrative, public or law enforcement body, or governmental, quasi-governmental, finance, tax, revenue, monetary, securities or futures exchange, court, central bank, agency, department or other authorities, or self-regulatory or industry bodies or associations of financial service providers or any of their agents with jurisdiction over all or any part of the Group (including the Payment & Clearing Association of China) or in any jurisdiction in so far as we need to do so to keep the relevant laws and regulations or any order, directive or request which we are required to keep to;

(vi) any persons acting on your or the relevant entity's behalf whose personal data are provided, payment recipients, beneficiaries, intermediaries, correspondent and agent banks, clearing or settlement systems, market counterparties, upstream withholding agents, or any persons making any payment into a customer's account;

(vii) in the event of payment collection, debt recovery or default, debt collection agencies;

(viii) any persons to whom we are or any member of the Group is under an obligation or required or expected to make disclosure for the purposes set out in, or in connection with, paragraphs 2(a)(viii) or 2(a)(ix) above;

(ix) any actual or proposed assignee(s) of ours or participant(s) or sub-participant(s) or transferee(s) of our rights in respect of you or the relevant entity(ies);

(x) business partners of ours, external services providers or any member of the Group for marketing, joint-marketing and research purposes, including the purposes set out in paragraphs 2(a)(iv) and 2(a)(v) above; and

(xi) a merchant or a member of a card association where the disclosure is in connection with use of a card.

(b) Such data may be transferred in and to a place outside Hong Kong, including jurisdictions with a lower level of data protection.

4 Biometric Data

(a) You should be aware that biometric data (which constitutes personal data) can be sensitive as it often contains an individual's physiological data with which an individual is born with (such as facial images) and behavioural data developed by such individual after birth (such as typing rhythm and voice pattern).

(b) Biometric data is not legally classified or categorised separately from personal data, but there are a few particular points regarding biometric data that we would like to bring to your attention:

(i) provision of your biometric data is not obligatory. If you do not want to provide your biometric data to us, you are free to do so, but that will mean that we may be unable to provide all or any part of our RD Wallet Services to you and/or the relevant entity(ies);

(ii) your biometric data will be used primarily for the purposes set out in paragraph 2(a)(ii) above;

(iii) your biometric data will in most cases be disclosed to the Transferees described in paragraphs 3(a)(iii) to 3(a)(v) only;

(iv) your biometric data may be relied upon by the relevant Transferees to take adverse actions against you, but you have the right to explain any irregularities concerning your biometric data before they do so;

(v) your right to request access to or correct your biometric data is set out in paragraph 7 below;

(vi) our collection and processing of biometric data is central to our and the relevant Transferees' client identification, client verification and anti-money laundering efforts;

(vii) a leak of biometric data could be very serious, but we will use all commercially reasonable efforts to ensure the security and integrity of your biometric data. Please refer to our Privacy Policy Statement for more information regarding our security practices; and

(viii) automated decision-making tools will be used in conjunction with biometric systems. These tools will automatically attempt to match your biometric data with other information regarding your identity. If the matching process fails, you will not pass our client identification and verification measures. You have the option of seeking human intervention by contacting us through any of the methods set out in paragraph 7(c).

5 Use of Personal Data in Direct Marketing

(a) We intend to use your personal data in direct marketing and we require your consent (which includes an indication of no objection) for that purpose. Please note that:

(i) your name, contact details, relationship with relevant individuals and relevant entities, location data, financial background and demographic data held by us from time to time may be used for marketing our own, other Group members' and/or our business partners'

products and services to you by email, letter, telephone, text messages or mobile application (e.g. targeted advertisements in-App and via WeChat push).

(ii) the following classes of products, services and subjects may be marketed:
   (1) payment, financial, banking and related products and services;
   (2) reward, loyalty, co-branding or privileges programmes and related products and services;
   (3) financial or banking products and services offered by our business partners; and
   (4) donations and contributions for charitable and/or non-profit making purposes;

(iii) the above products, services and subjects in sub-clause (a)(ii) may be provided by or (in the case of donations and contributions) solicited by us and/or:
   (1) any member of the Group or any agent or contractor engaged by the Group;
   (2) marketing or research services providers of us or any member of the Group;
   (3) business partners of us or any member of the Group (such as third party financial institutions and third party reward, loyalty, co-branding or privileges programme providers); and
   (4) charitable or non-profit making organisations;

(iv) in addition to marketing the above products, services and subjects ourselves, we may provide the personal data described in paragraph 5(a)(i) above to all or any of the persons described in paragraph 5(a)(iii) above for use by them in marketing those products, services and subjects; and

(v) we may receive money or other property in return for providing the personal data to the other persons in paragraph 5(a)(iv) above.

(b) If you agree to receive marketing communication but do not wish to receive them in the future, you may opt out of receiving them at any time, free of charge, by the following applicable means:-
   (i) following the unsubscribe instructions contained in the marketing text message;
   (ii) following the unsubscribe instructions or hyperlink in the marketing email;
   (iii) following the unsubscribe instructions in the mobile application;
   (iv) notifying us that you no longer wish to receive marketing communication when receiving our marketing calls; or
   (v) contacting us at the address stated in paragraph 7(c) below to tell us that you no longer wish to receive marketing communication through any channel.

6 Provision of Another Person's Personal Data

Where you provide to us personal data about another person (e.g. an individual, or a shareholder or director of your company), you must give to that person a copy of this Notice and, in particular, tell him/her that you have provided us with their personal data and how we may use his/her personal data.

7 Data Access Requests

(a) You have the right:
   (i) to check whether we hold personal data about you and to access such personal data;
   (ii) to require us to correct any personal data relating to you which is inaccurate;
   (iii) to ascertain our policies and practices in relation to personal data and to be informed of the kind of personal data held by us; and
   (iv) be informed on request which items of personal data are routinely disclosed to debt collection agencies and be provided with further information to enable the making of an access and correction request to the relevant debt collection agency.

(b) In accordance with the provisions of the Personal Data (Privacy) Ordinance, we have the right to charge a reasonable fee for the processing of any personal data access request.

(c) You should send requests for access to personal data or correction of personal data or for information regarding policies and practices and kinds of personal data held, by way of (i) completing an enquiry form on our website, (ii) messaging us using the messaging function in our mobile application, or (iii) writing by post or email to:

The Data Protection Officer
RD Technologies
Address: 16/F, Tower 535
No. 535 Jaffe Road
Causeway Bay
Hong Kong
Email: care@rd.group

(d) We will endeavour to use appropriate technical means to ensure that you can access, update and correct your personal data. In accessing, updating, correcting and/or deleting your personal data, we may ask for you to authenticate your identity in order to protect the safety of your personal data.

(e) To the extent permitted by relevant laws and regulations, we reserve the right to refuse unreasonable requests (for example, requests which may infringe or conflict with the privacy of others).

(f) Nothing in this Notice shall limit your rights as a data subject under the Personal Data (Privacy) Ordinance.

(g) Please contact us if you have any queries about this Notice.

(h) In case of discrepancies between the English and Chinese versions, the English version shall apply and prevail.

8 Residents of Mainland China

If you are within Mainland China, you will be additionally subject to Appendix 1 (China Personal Information Protection Policy) (附錄 1 (*中國個人信息保護政策*)). In the event of any inconsistency between this Notice (excluding Appendix 1) and the Privacy Policy Statement on one hand, and Appendix 1 on the other hand, the provisions which better allow us to comply with all the applicable laws and regulations, shall apply. This will, in most cases, be the provisions which impose a stricter standard on us.

9 Direct Marketing Consent

If you wish to amend your choice in relation to receipt of the latest promotion offers, services and product information of RD Technologies (including RD Wallet Technologies Limited and any member of our Group) and/or our business partners as set out in paragraph 5 of the this Notice, please visit the setting page in our mobile application to enable or disable the feature. You can change your decision at any time and at no cost. You can indicate the objection to the use of your personal data for direct marketing by disabling such feature on our mobile application. By

enabling such feature and selecting one or both channels of communication, you do not object to the use of your personal data for direct marketing in accordance with paragraph 5 of the Notice.

Appendix 1 - China Personal Information Protection Policy

This China Personal Information Protection Policy (**"Policy"**) is applicable to our group companies including but not limited to RD ezLink Limited, RD Wallet Technologies Limited, other affiliated companies and their respective successors and assigns (collectively, "**RD Technologies**" and "**we**", "**our**" or "**us**" shall be construed accordingly) and describes how we process your personal information if you reside in the People's Republic of China (the "**PRC**" or "China", which, solely for the purposes of this Policy, excludes Hong Kong SAR, Macao SAR, and Taiwan), pursuant to the laws and regulations of the PRC, Hong Kong SAR, and other applicable jurisdictions ("**Applicable Laws and Regulations**"). This Policy is written in English and Chinese language. In the event of any discrepancy between the English and the Chinese version, the Chinese version shall prevail.

Please read this policy carefully. Once you have read and agreed to the policy, you are deemed to have fully read, understood and agreed to the whole of the policy and consented to us to collect, retain, use and share your personal information in accordance with this policy. This policy, together with other terms and conditions implanted by us from time to time, apply to the products and services we provide.

The Policy will help you understand the following:

1. How We Collect and Use Your Personal Information

We may need to collect your personal information in order to provide you with our products and services ("**RD Products**"), which specifically refer to RD ezLink and RD Wallet that we provide to you, and the services of any type or nature that we provide to you users from time to time during your use of such products.

In this Policy, personal information refers to all kinds of information related to an identified or identifiable natural person recorded by electronic or other means, excluding anonymized information. Sensitive personal information refers to personal information that, once leaked or illegally used, is likely to infringe upon individuals' human dignity or endanger their health or property, including information on biometric identification.

Our business functions and the personal information that we collect to implement these functions are detailed below. If you refuse to provide your personal information to us, you may be unable to use the relevant services.

Please note that where you provide to us personal information about another person, please make sure that the person has read this policy and agreed to our processing of his/her personal information pursuant to this policy.

1.1 Account Administration Services We Provide

(1) Subject to the Applicable Laws and Regulations and regulatory requirements, when you create an RD Products individual user account, we will collect the following information from you in order to complete the account creation, identity verification and account management: **your name (in Chinese and/or in English, the same below), account name, password, age, date of birth, gender, identity information (e.g., China ID Card/passport, the same below), nationality, telephone number, email address, facial recognition information**, etc. During this process, we will verify your identity by sending a verification code via a text message or email. If you refuse to provide this information, you may be unable to create an individual user account or use our services normally.

(2) As required by the Applicable Laws and Regulations such as anti-money laundering, anti-terrorist financing, anti-fraud and sanctions, when you create an RD Products corporate user account on behalf of a company or with the authorization of a company and/or its shareholders, ultimate beneficiaries or directors, we will collect the following information about **the key individual person of the corporate user** (including shareholders, beneficial owners, de facto controller, legal representatives, directors, authorized signatories, account operators, etc.): **name, gender, identity information, date of birth, nationality, telephone number, e-mail address**, etc. If you refuse to provide the above information, you may be unable to create a corporate account or use our services normally. When you use our products/services, we will, from time to time, request you to provide proof of your authority to act on behalf of the business or of proper authorization.

(3) As required by the Applicable Laws and Regulations, and for security purposes, when we verify your account or when you log into your account, we will collect your account information, e.g., **username, password, photo and nickname**, to verify the validity of the username and password and assist you in retrieving your password if you forget it.

(4) **Please refer to the *Annex I: User Authorization Letter for Facial Recognition Service* for details of facial recognition information processing rules.**

1.2 Transfer Payment Services We Provide

(1) When you use the RD Products transfer and remittance function, we will collect **the name, account number, contact information** and the name of the transferee bank, and transfer notes; and we will also collect **account name, account number and contact information** of the transferor. In order to provide you with queries and convenient transfer services, we will collect and retain your transfer records.

(2) When you use the RD Products to make payments, we will collect your **name, account number, telephone number,** and text message verification code. To provide you with queries and convenient payment services, we will collect and retain your payment records.

1.3 Notices or Commercial Information We Send

(1) We may send you service status notices to keep you informed of your use of the RD Products or to familiarize you with our services.

(2) We will collect and use personal information such as **your name, telephone number, email address, interests, preferences, and feedback you provide in our research** to send you marketing, promotional, or other commercial information about our products and services, those of our affiliates and/or our business partners via email, letter, phone call, text messages, or push notifications. If you do not wish to receive such notifications or push notifications, you may opt out at any time by following the unsubscribe instructions in the app or by contacting us at the contact details stated in section 6 below.

1.4 Device Permissions We Request

In certain scenarios or services, we may request some of your device permissions to provide our services or improve your experience on RD Products. You may turn off some or all of the permissions in the device's settings, and refuse us collecting your personal information. The device permissions we may request to are listed in *Annex II*.

1.5 Technical Information We Collect

When you use the RD Products, we may collect your device particulars, including IMSI, IMEI, SEID, and collect your visits to RD Products through Cookies or similar technologies, e.g., online behavioral information, browser details, IP addresses and location information. Please refer to our Cookie Policy for more details about our use of cookies and similar technologies.

1.6 Our Cooperation with Third-Party Software Development Kit (SDK) Providers

In order to enable you to fully enjoy and use our products and services, RD Products are linked to SDKs from our authorized partners. We will urge these SDKs to comply with personal information protection obligations and we will strictly monitor these SDKs to protect the security of your personal information. The third-party SDKs we link to are listed in *Annex III*.

1.7 How We Use Your Personal Information

(1) Provide you with our products or services, including but not limited to, creating accounts, approving, managing, processing, or performing transactions or other services requested or authorized by you, and assisting us in designing, maintaining, supporting, and improving these products or services.

(2) Verify your identity the identity of relevant businesses, and conduct client due diligence, anti-money laundering, fraud detection, and transaction monitoring on you and relevant businesses.

(3) Fulfill our compliance responsibilities, including statutory obligations under the Applicable Laws and Regulations, judgments, court orders or requests of any regulatory, governmental or other authorities, such as the obligation to make reports to the relevant authorities.

(4) You authorize us to collect and use your information on an ongoing basis during the period in which we provide our services to you. When you cancel the service, we will stop collecting your relevant personal information, but we will continue to use your relevant personal information previously collected in the areas of business data archiving, auditing, assistance with regulatory investigations, fulfillment of anti-money laundering and sanction regulations, etc., in accordance with Applicable Laws and Regulations and regulatory requirements.

(5) Assist us and our partners with detecting, preventing and investigating crimes and safeguarding public interests.

(6) Communicate with you and the relevant businesses.

(7) To use your personal information to assist actual or proposed business or asset transferees and participants in business or asset sales transactions to evaluate the operations related to such business and/or assets.

(8) To improve your product or service experience or to prevent risks, we may aggregate, statistically analyze, and process service usage, but this information will not contain any identifying information about you.

(9) We may analyze your personal information to better help us understand your needs, behaviors, preferences, interests, experiences and habits in order to provide you with products and services that may be of interest to you.

(10) Any other use that you have authorized or agreed to or that is permitted by the Applicable Laws and Regulations.

1.8 Exceptions for us to obtain consent for the collection and use of your personal information

Pursuant to the Applicable Laws and Regulations, we may collect and use your personal information without your consent under the following exceptions:

(1) where it is necessary for the conclusion or performance of a contract to which you are a party;

(2) where it is necessary for our performance of statutory duties or obligations;

(3) where it is necessary to deal with public health emergencies or for the protection of life, health, and property safety of individuals in emergencies;

(4) Unless you explicitly refuse, where personal information is collected within a reasonable scope from information that has legally and publicly disclosed by you or other means, such as legal news reports, information disclosed by government and other channels, etc., pursuant to the Applicable Laws and Regulations;

(5) Other circumstances as provided by the Applicable Laws and Regulations.

2. How We Retain and Protect Your Personal Information

2.1 Period and Place of Retention

Personal information that we collect and generate in China is stored in the server located in Hong Kong. We will retain your personal information only for a limited period of time needed to fulfil the purposes of processing stated in the Policy. After the expiration of the retention period, your personal information will be deleted or anonymized via a reasonable method. Subject to the Applicable Laws and Regulations, the retention period will depend on following standards and the longest period of time shall govern.

(1) perform business functions that you agree to use;

(2) ensure the safety and quality of our services;

(3) longer retention period as you agreed;

(4) whether there is any other special agreement on the retention period.

As we provide our products and services from servers located in Hong Kong, you understand that we may transfer, retain and process your personal information in/between our affiliates, partners and service providers worldwide. In these circumstances, we will comply with the Applicable Laws and Regulations and take appropriate measures to ensure that your personal information is adequately protected.

2.2 How We Protect Your Personal Information

(1) We have implemented industry-standard security technical measures, to protect your information from unauthorized access, duplication, public disclosure, use, modification, transfer, damage, or loss. For example, we will implement encryption technologies to ensure the confidentiality of data, implement trusted protection mechanisms to protect data from malicious attacks, implement access control mechanisms to restrict the access, and we will monitor the access and the processing of information systematically to ensure that only authorized personnel have access to the personal information. We will also take all other reasonable and practicable management measures to ensure the security of your personal information.

(2) We will take reasonable efforts to ensure the security of the personal information you provided. **Please also be sure to keep your account name and other identification information properly. We will identify you by your account name and other identification information when you use our services. Once you disclose the aforesaid information, you may suffer losses which may result in adverse legal consequences. If you find any possible or actual disclosure of your account name and/or other identification information, please contact us immediately, we may take measures to avoid or reduce the losses.**

(3) If a personal information security incident unfortunately occurs, we will take immediate and effective remedial measures to prevent the security incident from spreading, as required by the Applicable Laws and Regulations. We will inform you of the incident in a timely manner by email, letter, telephone and/or push notification. If it is difficult to inform you one by one, we will issue the announcement in a reasonable and efficient manner. Meanwhile, we will also proactively report the handling of personal information security incidents in accordance with the requirements of regulatory authorities.

(4) Please understand that the internet environment is not entirely safe, even though, we will do everything possible to ensure the security of your information. However, due to limitation of technology development and other objective factors, as well as different malevolent means that may exist in the internet environment, it is impossible to constantly ensure complete security, even if all precautions are taken.

3. How We Disclose Your Personal Information

3.1 Entrusted Processing

To provide our products and services to you, we may entrust third-party service providers to offer operation and service support, during which we may disclose information with such service providers who provide services on our behalf and follow our instructions, to realize functions of our products and services, including but not limited to the authentication service providers, marketing or research service providers, message service providers, software/system technology service providers, data analytics companies and system server hosting companies, etc. We do not authorize such service providers to use or disclose your personal information, except to the extent necessary in order to perform services on our behalf or it is necessary for us to comply with legal requirements.

3.2 Sharing

(1) Sharing with your consent or at your authority

Upon your consent, we will provide your personal information to other parties. You consent that we share your necessary personal information with our affiliates and who shall process personal information subject to the purposes in this Policy. We will re-obtain your consent if our affiliates intend to change the purpose of the processing of your personal information. We may share your information with our partners and other third parties in order to provide better services to you. We will only share your personal information for lawful, legitimate and necessary purposes and will only share such personal information as is necessary to provide complete services to you. Our partner is not entitled to use the personal information beyond the scope of purpose.

(2) Sharing required by the Applicable Laws and Regulations

We may share your personal information pursuant to the Applicable Laws and Regulations, or in accordance with compulsory requirements of competent government authorities, tax, monetary, securities or futures exchange, court, central bank, self-regulatory or industry associations or other authorities.

3.3 Public disclosure

We will not disclose your personal information publicly, except under the following circumstances:

(1) After obtaining your explicit consent;

(2) In accordance with the Applicable Laws and Regulations, legal procedures, the requirements of litigation or in order to fulfill our legal obligations, we may disclose your personal information.

4. Your Rights

4.1 Access and Copy Your Personal Information

You have the right to request to access and copy your personal information, pursuant to the Applicable Laws and Regulations.

4.2 Correct and Supplement Your Personal Information

If you notice that the personal information we processed is incorrect or incomplete, you have the right to request us to correct or supplement such personal information.

4.3 Delete Your Personal Information

Under the following circumstances, you may request to delete your personal information:

(1) The processing purpose has been achieved or cannot be achieved, or it is no longer necessary to achieve the processing purpose;

(2) We cease the provision of products or services, or the retention period has expired;

(3) You withdraw the consent;

(4) We process personal information in violation of any Applicable Laws and Regulations or the agreement;

(5) Other circumstances as provided by the Applicable Laws and Regulations.

If the retention period provided by the Applicable Laws and Regulations have not expired, or it is difficult to technically delete the personal information, we will cease the processing of such personal information other than the retaining and taking the necessary security protection measures.

4.4 Withdraw Your Consent

If you intend to amend or withdraw your consent to our processing of your personal information, you can contact us via the contact methods in this Policy. We will no longer process your personal information if you withdraw your consent. However, the withdrawal of your consent will have no impact on the personal information processing activities that were previously carried out with your consent.

4.5 Delete Your Account

You have the right to request the deregistration of your account, and we will delete your account subject to the Applicable Laws and Regulations.

4.6 Respond to the Above-mentioned Request

(1) You can contact us via the contact methods in this Policy if you want to exercise the aforementioned rights or if you require us to explain the provisions of this Policy. We will reply within 15 working days.

(2) You may be required to submit a written request or other way to verify your identity. We may ask you to verify your identity before we process your request.

(3) In accordance with the requirements of the Applicable Laws and Regulations, we will not be able to respond to your request under the following circumstances, but we will explain to you:

(a) In connection with our fulfillment of obligations stipulated by Applicable Laws and Regulations and regulatory provisions;

(b) Directly related to national security and national defense security;

(c) Directly related to public safety, public health, and major public interests;

(d) Directly related to the criminal investigation, prosecution, trial and execution of sentences;

(e) There is sufficient evidence to proof that you have subjective malice or abuse of rights;

(f) For the purpose of protecting your or other people's life, property and other significant legitimate rights and interests, but it is difficult to obtain individual's consent;

(g) Responding to your request will cause serious damage to the legitimate rights and interests of you or other individuals or organizations;

(h) Involving trade secrets.

5. How to Update this Policy

We may revise this Policy from time to time. We will notify you when this Policy is updated, as the case may be, via pop-ups, email notifications, website announcements, etc.

6. How to Contact Us

If you have any questions, comments or suggestions about this Policy, you can contact us at any time by writing post or email to RD Technologies (the Data Protection Officer), which address is 16/F, Tower 535, No. 535 Jaffe Road, Causeway Bay, Hong Kong, or email to care@rd.group.

Annex I: User Authorization Letter for Facial Recognition Service

Dear user,

RD Technologies ("**we**", "**our**" or "**us**") is well aware of the importance of facial recognition information to you and will do our best to keep your facial recognition information safe and secure. **Before you consent to this authorization letter, please read the terms and conditions carefully and pay attention to your rights and obligations.**

1. **When you register RD Products, we may require you to verify your identity by means of facial recognition technology, for the purpose of registering and managing your account, verifying and maintaining the security of your personal information and account, conducting customer due diligence, safeguarding transaction security, controlling risk, etc., or as required by Applicable Laws and Regulations in situations where customer identity verification is mandatory.**

2. **You authorize us to retain your facial recognition information for such period of time as is necessary for us to achieve the foregoing purposes.**

3. With your consent and verification of your, your facial recognition information will be archived and stored encrypted in our back-end database. We will use industry-standard security measures to protect the data from unauthorized access, public disclosure, use, modification, damage or loss.

4. For facial recognition, we will collect your facial recognition information (including facial image and online videos) and the facial recognition information involved in the identity certificates you upload on RD Products, and we will compare such information on our RD Products with the information stored by any agency permitted by Applicable Laws and Regulations or authorized by governmental authorities, or with the facial recognition information you provide.

5. **Please note that facial recognition information is only used as an auxiliary method by which we verify your identity and should not be considered the sole means of identification. It is not necessary for you to provide your facial recognition information. However, if you refuse to provide such information, you may be unable to use the corresponding services.** If the facial recognition verification is not successful, you may reinitiate the verification after adjusting light, distance or angle, or select another verification method we provide to complete the identity verification (if any).

6. In principle, we will not disclose your facial recognition information to any third party. However, we may provide your facial recognition information to providers of customer due diligence and sanctions/anti-money laundering/anti-fraud service/data processing/security service and other services, to our affiliates, or pursuant to regulatory provisions under applicable laws and regulations, or as compulsorily requested by government authorities, tax authorities, monetary, securities or futures exchanges, courts, central banks, self-regulatory or industry associations or other institutions, for business purposes, or by the requirements of applicable laws and regulations or other reasons. **By consenting to this authorization letter, you are deemed to have agreed that we may share your facial recognition information with such third parties.**

7. We attach great importance to the protection of your privacy and will protect and regulate personal information, such as facial recognition information, collected under this authorization letter in strict accordance with the Personal Information Collection Statement in respect of RD ezLink or RD Wallet and the appendix "*China Personal Information Protection Policy*" as updated from time to time.

8. **You understand and agree that this authorization letter shall be effective upon your review and consent.**

Annex II: List of Requested Device Permissions

Device Permissions	Request purpose	Consequence of close/refusal
Device status	Verification of the device ID to secure the login of the account to which the device is bound	Inability to access the RD Product
Storage	To cache the text, images, and video generated during your use of the Platform	Inability to use the text, images, and video function
Camera	ID card recognition, passport recognition, bank card recognition, QR code recognition, facial recognition, avatar setting, video recording, AR, photo taking, scanning, and to be used in enhanced authentication via facial recognition, avatar setting, video recording scene and social sharing	Inability to use the camera function
Photos	Use as your avatar or a remark for your transaction information, and to be used in facial recognition and social sharing features	Inability to use the photos function
Microphone	Voice recording, AI interaction, voice customer service, connection with the account manager and facial recognition	Inability to use the microphone function
SMS	Sharing of URLs via SMS	Inability to use the SMS function
Location	Conduct customer due diligence, transaction monitoring, push notification, social sharing and presentation of urban services	Inability to use the location function
Network connection	Connection with the server	Inability to use the network connection function
Application list	Risk control and prevention of fraudulent transactions	None
Calendar	Scheduling of transactions and to-do reminders	Inability to use the calendar function
Notifications	Receive notifications in the process of account opening, making transactions, etc.	Inability to receive notifications
Address book	Auto-fill payee information based on phone numbers and email addresses from address book	Inability to auto-fill payees' phone numbers and email addresses

Annex III: List of Third-party SDKs

Categories of SDK	Types of personal information collected	Purpose of personal information collected
Statistical SDK	Personal device(s) information, including user activity of different applications on such device(s)	To conduct business data analysis and users' identification for improving accuracy and delivery rate of notifications
Push SDK	Personal network and location data, for example, IP address, wireless network data and cable landing station data	To improve servers' network connection stability and continuity and enable regional push notification functionality
Push SDK	List of applications installed on personal device(s)	To enable intelligent push notification functionality for reducing unnecessary notifications
Identity verification SDK	Personal identity information, including photos and videos	To verify users' identity

Version: March 2024