

Privacy Policy

1. Introduction

WizWiz and the related Appen crowd contributor platform, mobile applications and websites (collectively, the “Platform”) are owned by APPEN SINGAPORE PTE. LTD. (UEN 202554404E), with registered address at 6 Shenton Way, #33-00, OUE Downtown, Singapore 068809 (“Appen Singapore”, “we”, “us” or “our”). The Platform may be operated, administered or supported by Appen Singapore and/or Appen affiliates, including Appen entities located in China, for platform operation, project management, technical support, compliance, recruitment/project invitation, payment administration and related business purposes.

We are fully aware of the importance of personal information to you and will do our utmost to ensure the security and reliability of your personal information. We are committed to maintaining your trust and adhering to the principles stipulated in the relevant laws, regulations, and technical standards to protect your personal information: the principle of consistency of rights and responsibilities, the principle of clear purposes, the principle of choice and consent, the principle of minimum necessity, the principle of openness and transparency, the principle of ensuring security, and the principle of subject participation, etc. At the same time, we promise to take corresponding security protection measures in accordance with the mature security standards of the industry to protect your personal information. Please read and understand this Privacy Policy carefully before using our products (or services), and we will collect, process, and disclose your information in accordance with this policy.

Before you start using our products and services, you must carefully read and understand this policy, especially the terms highlighted in bold. These terms are important, and we want to make sure you fully understand and agree to them before you proceed. We have tried to explain any specialized terms in this policy in a simple and easy-to-understand way. If you have any questions, comments or suggestions about this policy, you can contact us through the various contact details provided in this policy.

This Privacy Policy is designed to remind you to read it when you visit, install, register or use the Services for the first time, and fully discloses the functional scenarios related to your Personal Information in this Privacy Policy to let you know how your Personal Information is collected, used, shared so that you have the right to independently decide whether to authorize and the scope of authorization.

When you use our Services, or when processing your Personal Information in connection with those Services, we will be the data controller of such Personal Information. We respect your right of choice and refusal, and provide convenience for your choice and refusal, we will not set up obstacles to your right of choice or refusal, and will not mislead you to agree through improper means such as fraud and deception to collect Personal Information; we will not bypass your authorization to obtain your Personal Information through concealed technical means, including but not limited to enabling end user’s authorization by default, stealing end user’s privacy through malicious acts such as clipboard hijacking, eavesdropping, and screen recording.

For the purposes of the Singapore Personal Data Protection Act 2012 (“PDPA”), Appen Singapore is the organisation responsible for personal data collected through the Singapore Platform. Where applicable, Appen Singapore may also act as a controller or processor under

other applicable data protection laws depending on your jurisdiction and the relevant project.

2. Scope of Privacy Policy

This Privacy Policy explains and describes: When this Privacy Policy applies. Below are the following Sections of this Privacy Policy:

- 1) When this Privacy Policy Applies
- 2) Our Use of Cookies
- 3) What Kinds of Your Personal Information We Will Collect and How to Collect
- 4) Legal Basis for Usage of Personal information
- 5) Use of Information
- 6) Disclosure of your Information
- 7) Transfer of your information
- 8) Retention of Your Data
- 9) Links to Other Websites
- 10) Collection of Anonymous Information
- 11) Information Security
- 12) International Transfers
- 13) Personal Information Protection for Minors
- 14) Your Rights
- 15) Feedback, Including Comments, Questions and Complaints
- 16) Changes to the Privacy Policy
- 17) General Disclaimers
 - a) KYC and identity verification
 - b) Payment processing and payment records
 - c) Access by Appen affiliates and service providers
 - d) Data breach and security incident handling

3. When this Privacy Policy Applies

This Privacy Policy applies to the following scenarios:

- 1) where you use any of our Services;
- 2) where you register for, apply for, accept or perform contributor tasks, projects or other services through the Platform;
- 3) where your supply of services to us involving any your Personal Information;
- 4) where as a result of your relationship with one or more of our clients; and/or
- 5) where any information collected from third parties.

4. Our Use of Cookies and Similar Technologies

We use only strictly necessary cookies and similar technologies that are required to provide, secure and operate the Platform. These may be used for purposes such as login, authentication, session management, security, fraud prevention, troubleshooting, maintaining user sessions, remembering essential settings, and enabling core Platform functionality.

We do not use cookies or similar technologies for advertising, marketing, user profiling, cross-site tracking or non-essential analytics.

Because these cookies and similar technologies are necessary for the Platform to function properly, they cannot be disabled through our Platform settings. You may block or delete cookies through your browser or device settings, but doing so may affect your ability to access or use some or all Platform functions.

If we introduce non-essential cookies or similar technologies in the future, such as advertising, marketing, profiling, cross-site tracking or non-essential analytics cookies, we will update this Privacy Policy and, where required by applicable law, provide appropriate notices, preference settings and/or consent mechanisms.

5. What Kinds of Your Personal Information We Will Collected and How to Collect

“Personal Information” is any information that can be used to identify you or that we can link to you. When you visit,download, install or use the Application, Appen may use automatic means (including, for example, cookies and web beacons) to collect information about your Device and about your use of the Application. You also may be required to provide certain information about yourself as a condition to visiting, downloading, installing or using the Application or certain of its features or functionality, and the Application may provide you with opportunities to share information about yourself with others.

1) List of personal information collected

Use case	Purpose	Collection method	Personal data
Registration and login	Account creation, identity/account management, Platform access	User input / Platform systems	First name, last name, email address, country/region, language(s), username/nickname, login credentials/authentication data
Optional profile	Matching contributors with suitable projects	User input	Industry field, position, years of work experience, degree, school, major and other optional profile fields, where provided
KYC / identity verification	Identity verification, fraud prevention, account security, compliance and payment support	Didit KYC page / vendor backend / Appen access to vendor results	Country, identity document type, identity document/passport images, facial images, verification result/status, verification logs and related KYC information
Payment processing	Payment of accepted contributor fees	User input / Payoneer or designated payment provider / Platform payment records	Name, payment provider account details/identifier, payment status, payment history, monthly revenue statement, currency, task fees, payment error records and compliance/payment support records
Task participation	Task performance, review, acceptance, quality control, client project delivery	User submission / Platform	Task responses, annotations, labels, translations, transcriptions, evaluations, photos, videos, audio recordings, survey responses, location-specific task data and other deliverables
Location-based tasks	Confirming task location where required by project terms	Device permission / app detection	GPS/location data for relevant tasks only
Device and technical	Security, fraud prevention, troubleshooting, platform	Platform/app/SDK systems	Device ID, IP address, operating system, device model, logs, app

Use case	Purpose	Collection method	Personal data
data	operation, analytics/statistics and technical support		version, error reports, app list/installed application information where strictly necessary
App permissions	Enabling relevant task functions	Device permission process	Camera, microphone, album/photo library, location and other permissions required for specific tasks
Support and complaints	Responding to queries, complaints, access/correction/deletion requests and disputes	User communications / support records	Name, email, request details, complaint details, correspondence and handling records

2) Device Permission Call List

Name of Device	Introduction	Purpose
Installed APP Information	Obtain the list of currently installed applications on the phone	Used only where necessary for fraud prevention, security, compatibility checks or SDK operation
Sensor	Obtain orientation sensor	To help you adjust the screen rotation direction
Microphone	Capture audio when obtaining audio	For you to complete audio collection tasks
Camera	Use the camera to take photos or videos	To help you complete photo or video collection tasks
Album	Access the local album	To access the photos or videos stored in the album after you have completed the collection task
Location	Use the location information	Ensure user on site when collecting data
safetynethelper	Obtain device serial number	Obtain device information
com. learnium	Obtain ANDROID_ID	Obtain device information

com. reactnative community	Obtain device MAC address, obtain device IP address, software installation list, WIFI_BSSID	Obtain device information
async-storage	Obtain device MAC address, obtain device IP address, software installation list, WIFI_BSSID	Obtain device information

3) Information Shared with Third Party

Third party / recipient	Purpose	Personal data
Didit	KYC / identity verification	Identity document/passport images, facial images, country, document type, verification status/results and related KYC information
Payoneer or designated payment provider	Contributor payment processing	Name, payment account details, payment amount, currency, payment status and payment-related identifiers
Alibaba Cloud Singapore	Hosting, storage, backups, logs, cloud infrastructure and security	Platform data, account data, task data, technical logs, backups and related personal data hosted in Singapore
Appen China R&D team	Issue investigation, troubleshooting, data statistics/analysis, technical support	Contributor personal data, task/project data, logs and platform data necessary for those purposes
Appen China recruitment team	Identifying and inviting suitable candidates for recruitment or project opportunities	Contributor profile, language, country/region, task/project suitability and contact data
Appen affiliates	Platform operation, support, compliance, project management, payment administration and business administration	Personal data necessary for the relevant purpose
Professional advisers / authorities	Legal, regulatory, audit, dispute, investigation or compliance purposes	Personal data relevant to the request or matter

Products or services provided by third parties are operated by the relevant third parties. When you use these products or services, they may also collect your information. We do not store or access personal information collected in this manner and are not responsible for how third parties use the personal information they collect from you. We also cannot control their use. Our Privacy Policy does not apply to products or services provided by third parties that are

linked through our services.

Therefore, we strongly recommend that you take the time to carefully read the privacy policies of the relevant third parties to determine whether to use the service. The relevant third parties shall independently bear the responsibility for the services they provide and the security of the data. Any disputes arising from the third-party service or its use of your information, or any violations of relevant laws and regulations by the third-party service, or any losses you may suffer in the process of using the third-party service, please resolve with the third party.

We follow the principles of personal information minimization and purpose limitation, and only collect and use the minimum personal information necessary to provide Services. We will not collect and use unique device identifiers unless it is necessary to use the Services, and prefer to use other resettable and deactivable device identifiers.

Access by Appen China teams is logged, role-based and revocable. Personal data is stored in Singapore, but authorised personnel located outside Singapore may remotely access it for the purposes described in this Privacy Policy.

4) Other Purposes and Uses

We will seek your consent in advance if we use personal information for purposes not specified in this statement and policy, or if we use information collected for a specific purpose for other purposes.

5) According to the relevant laws and regulations, we do not need to obtain your consent for the collection of your personal information in the following circumstances:

- a) Directly related to national security and defense security;
- b) Directly related to public security, public health, and major public interests;
- c) Directly related to criminal investigation, prosecution, trial, and the execution of judgments, as well as other judicial or administrative law enforcement activities;
- d) Necessary to safeguard your or another individual's significant legitimate rights and interests, such as life and property, when it is difficult to obtain your consent;
- e) The personal information collected is information that you have voluntarily disclosed to the public;
- f) Collected from information that has been lawfully disclosed to the public, such as through legitimate news reports or government information disclosure channels;
- g) Necessary for the conclusion and performance of contracts or other written agreements at our request;
- h) Necessary to maintain the secure and stable operation of the products and/or services provided, such as identifying and addressing faults in the products and/or services;
- i) Related to our compliance with the obligations stipulated by laws and regulations;
- j) Other circumstances stipulated by laws and regulations.

Please be informed that, in accordance with the applicable laws, if we take technical and other necessary measures to process personal information so that the data recipient cannot re-identify a specific individual and cannot restore the original data, or if we may conduct de-identified research, statistical analysis, and prediction on the collected information to improve the content and layout of the platform, and enhance our products and services (including using anonymized data for machine learning or model algorithm training), then the use of such processed data does not require

separate notification to you and your consent.

If we cease the operation of the products or services of this platform, we will promptly stop the activities of continuing to collect your personal information, notify you of the cessation of operations in the form of individual delivery or announcement, and delete or anonymize the personal information we hold.

6. Legal Basis for Usage of Personal Information

Where we intend to use your personal information, we rely on the following legal grounds:

- 1) **Performance of a contract:** we may need to collect and use your Personal Information to enter into a contract with you or to perform a contract that you have with us.
- 2) **Legitimate interests:** where we consider use of your information as being (a) non-detrimental to you, (b) within your reasonable expectations, and (c) necessary for our own, or a third party's legitimate purpose, we may use your Personal Information for:
 - a) our own direct marketing or continued communication
 - b) the prevention of fraud;
 - c) our own internal administrative purposes;
 - d) ensuring network and information security, including preventing unauthorised access to electronic communications networks and stopping damage to computer and electronic communication systems;
 - e) reporting possible criminal acts or threats to public security to a competent authority.
- 3) **Compliance with a legal obligation:** We may be required to process your information due to legal requirements, including employment laws, tax laws and other regulatory provisions applicable to us.
- 4) **Consent:** You may be asked to provide your consent in connection with certain services that we offer, for example in respect of any processing of your personal information for our marketing purposes where you or your employing organisation is not our client, or in respect of certain special categories of personal information such as your health or racial background for which we are legally obliged to gain your consent due to the sensitive nature of such information and the circumstances in which it is gathered or transferred. Where we are reliant upon your consent, you may withdraw this at any time by contacting us in accordance with the Section 17 (*Feedback*) below.

For users whose personal data is subject to the Singapore PDPA, we collect, use and disclose personal data where you have consented, where deemed consent applies under applicable law, where the collection/use/disclosure is necessary to perform or enter into a contract with you, where required or authorised by law, or where another exception under the PDPA applies. We will notify you of the purposes for which your personal data is collected, used or disclosed, unless an exception applies.

7. Use of Information

We use personal data to:

- 1) create, verify, administer and secure your Platform account;
- 2) conduct KYC/identity verification through Didit or other approved vendors;

- 3) assess eligibility for tasks and project opportunities;
- 4) send task emails, project invitations and app push notifications;
- 5) administer, review, accept, reject and quality-check task submissions;
- 6) maintain monthly revenue statements and payment records;
- 7) process payments in USD through Payoneer or another designated payment provider;
- 8) provide technical support, troubleshooting and account support;
- 9) investigate fraud, abuse, security incidents, policy breaches or unauthorised access;
- 10) maintain platform security, logs, backups and analytics/statistics;
- 11) comply with legal, tax, accounting, audit, regulatory and dispute-resolution obligations;
- 12) respond to access, correction, deletion, withdrawal, complaint and support requests; and
- 13) improve Platform functionality and project operations.

We do not send SMS marketing or email marketing through the Platform. Task emails, app push notifications and project invitations are service or Platform communications.

We may not be able to do some or all of these things listed above without your personal information. Sometimes we may need to give information to our agents and subcontractors who assist us in providing services. In these circumstances we always ensure that the information is safe and secure. If at any time we intend to change the purpose for which we hold your personal information, for example to offer you with a complimentary service that we may provide in the future, we will give you prior information of that new purpose so you are aware of this. Subject to the above, the information collected about you will not be used for any other purposes and will not be sold or otherwise disclosed to any other organisations, unless required by law, except our successors in title.

8. Disclosure of Your Information

We may, in providing our services and operating our business, allow access to your personal information to the different entities within our group for our internal administrative purposes such as billing, promoting our events and services, and providing you or your organisation with services, provided in all instances that such processing is consistent with this Privacy Policy and applicable law.

We may exchange your personal information with third-party service providers contracted to us where any of the following apply:

- 1) You have consented to us sharing your personal information in this way.
- 2) We deem reasonably necessary to provide you with the services that you have required at any particular time.
- 3) Such sharing is provided for under contract, including our terms and conditions for any particular service that we may provide to you.
- 4) Such sharing is to law enforcement bodies or other government authority.
- 5) We need to enforce or apply our terms and conditions to which you have agreed (or other terms that have been agreed to apply to our relationship with you or your employing organisation).
- 6) It is necessary to protect the rights and interests, property, or our safety or the safety of our clients or others.
- 7) It is relevant in the circumstances to disclose the information to parties with whom we have co-promotional arrangements (such as jointly sponsored events, external venues, or caterers).
- 8) Our agents or contractors who assist us in providing our services require such

information, for example in fulfilling requests for information, receiving and sending communications, updating marketing lists, analysing data, providing support services or in other tasks from time to time. Our agents and contractors will only use your information to the extent necessary to perform their functions.

- 9) All, or most, of our assets are merged with or acquired by a third party, or we expand or re-organise our business, in which case your personal information may form part of the transferred or merged assets.
- 10) We are under a legal, regulatory or professional obligation to do so (for example, in order to comply with a Court Order).

Any third parties that we may share your data with are obliged to keep your details securely, and to use them only to fulfil the service they provide you on our behalf. When such third parties no longer need your personal information to fulfil this service, they will dispose of such details in line with our policy unless they are themselves under a legal obligation to retain the information. If we wish to pass your sensitive personal information onto a third party we will only do so once we have obtained your consent, unless we are legally required to do otherwise.

We own the database rights in the information collected via our online services. We do not sell, rent, or otherwise share information that reasonably identifies you or your organisation with unaffiliated entities for their independent use except as expressly described in this Privacy Policy or with your express prior permission. We may share information that does not reasonably identify you or your organisation as permitted by applicable law.

Appen Singapore may disclose or make personal data available to Appen affiliates, including Appen entities and teams located in China. The Appen China R&D team may access data through the Appen backend and Alibaba Cloud backend/console for issue investigation, troubleshooting and data statistics/analysis. The Appen China recruitment team may access data for identifying and inviting suitable candidates to participate in recruitment or project opportunities. Such access is intended to be logged, role-based and revocable.

9. Transfer of your information

We will not sell your personal data. We may transfer personal data as part of a merger, acquisition, restructuring or transfer of business/assets, provided that the recipient is required to continue protecting the personal data in accordance with this Privacy Policy or applicable law. We may also disclose, transfer or make personal data available to Appen affiliates and service providers for the purposes described in this Privacy Policy.

10. Retention of Your Data

We retain personal data only for as long as reasonably necessary to fulfil the purposes for which it was collected, or as required or permitted for legal, tax, accounting, audit, security, fraud-prevention, dispute-resolution, payment, regulatory or compliance purposes.

Personal data collected through the Singapore Platform will be stored on servers located in Singapore, including Alibaba Cloud Singapore. Platform databases, backups and logs are intended to remain in Singapore.

When you delete your account, we will delete or anonymise personal data stored on the Platform, except where retention is required or permitted for legal, tax, accounting, audit,

security, fraud-prevention, dispute-resolution, payment, regulatory or compliance purposes, or where deletion is technically implemented through backup deletion cycles.

11. Links to Other Websites

The Application, Site and communications may, from time to time, contain links to and from the websites of our partner networks, advertisers and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal information to these websites. This Privacy Policy does not cover the information practices of those third-party websites.

The Platform may redirect you to third-party pages or services, including KYC/identity verification pages operated by Didit and payment services operated by Payoneer or another designated payment provider. Such third parties may process your personal data under their own terms and privacy notices. Where Appen Singapore determines the purposes of processing or receives/accesses your information from such vendors, Appen Singapore will process such information in accordance with this Privacy Policy.

12. Collection of Anonymous Information

We sometimes collect anonymous information from visits to an Application and a Site to help us provide better customer service. For example, we measure visitor activity on the Sites, but we do so in ways that keeps the information anonymous. We use the information that we collect to measure the number of visitors to the different areas of our Sites, and to help us make our Sites more useful to visitors. This includes analysing these logs periodically to measure the traffic through our servers, the number of pages visited and the level of demand for pages and topics of interest. None of the information constituted in such logs will include or constitute personal information and such logs may be preserved indefinitely and used at any time and in any way to prevent security breaches and to ensure the integrity of the data on our servers.

13. Information Security

We take steps to hold information securely in electronic or physical form.

We use organisational and technical measures designed to protect personal data against unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. These measures may include access controls, role-based permissions, logging, encryption or encrypted transmission, vendor controls, security monitoring, backup controls and incident-response procedures. Access by Appen China teams is intended to be logged, role-based and revocable. Our information security policy is supported by a variety of processes and procedures, and we store information in access-controlled premises or electronic databases requiring logins and passwords. All of our employees, officers or contractors and third-party providers with access to confidential information are subject to access controls and confidentiality obligations, and we require our third-party data storage providers to comply with appropriate information security industry standards. Whilst we continually strive to ensure that our systems and controls are updated to reflect technological changes, the transmission of information via the internet is not completely secure, and as such we cannot guarantee the security of your data transmitted to our online services which is at your own risk. It is your responsibility to scan what you choose to download from our Sites to ensure that it is free of

such items as viruses, worms, Trojan horses and other similar destructive code. If you communicate with us using a non-secure mechanism, you assume the risks that such communications between us are intercepted, not received, delayed, corrupted or are received by persons other than the intended recipient. Once we have received your information, we will take reasonable steps to use procedures and security features to try to prevent unauthorised access, modification or disclosure. You can help us to keep your information secure by ensuring that any user name or password in relation to our online services is kept strictly confidential to you and not be made available to any other person. You should stop using your username and password and notify us immediately if you suspect that someone else may be using your user details or password. If we become aware of a data breach or suspected data breach, we will assess and respond to the incident in accordance with applicable law. Where the PDPA requires notification to the Personal Data Protection Commission and/or affected individuals, Appen Singapore will take steps to provide the required notification.

14. International Transfers

Personal data collected through the Singapore Platform will be stored in Singapore. However, Appen Singapore may allow authorised Appen affiliates and service providers located outside Singapore, including Appen teams located in China, to remotely access or process personal data for Platform operation, project management, issue investigation, troubleshooting, data statistics/analysis, recruitment/project invitation, technical support, compliance, security, payment administration and related business purposes.

Where personal data is transferred to, accessed from or processed in a country or territory outside Singapore, Appen Singapore will take steps required under applicable data protection laws, including the Singapore PDPA, to ensure that the recipient is bound by legally enforceable obligations or other appropriate safeguards to provide a standard of protection comparable to the protection under the PDPA.

15. Personal Information Protection for Minors

The Platform is not intended for individuals under 18 years old. We do not knowingly allow individuals under 18 to register for or use the Platform. If we become aware that an individual under 18 has provided personal data through the Platform, we may delete the account and related personal data, subject to applicable legal and compliance requirements.

16. Your rights

Subject to applicable law, you may request access to personal data we hold about you, request correction of inaccurate or incomplete personal data, withdraw consent, request deletion of your account, or make a complaint about our handling of your personal data. We will respond to access, correction, deletion and privacy complaint requests within a reasonable time and, where applicable, within 30 days.

Under applicable data protection legislation, we have a duty of care to ensure that your personal information is accurate and up to date. Therefore, please contact us to update or correct your information if this changes or if you believe that any information that we have collected about you is inaccurate at the contact details below.

Where you have consented to our processing of certain personal information, you can at any

time withdraw such consent and/or tell us not to contact you with updates and information regarding our products and services (or part of them) either at the point such information is collected, (using an appropriate acknowledgment and consent) or, where you do not wish us to continue to use your information in this way, by following the unsubscribe instructions on any communications sent to you. You can also exercise this right at any time by contacting us using the contact details below.

You can request:

- 1) access to the personal information we hold about you;
- 2) corrections or updates to your details;
- 3) the erasure of your Personal Information;
- 4) the portability of personal information that you have provided to us in a structured, commonly used and machine-readable format.
- 5) You can change the scope of your authorized consent by deleting information, disabling device functions, adjusting privacy settings on the platform, or other similar means to alter the scope of your authorization for us to continue collecting personal information or to withdraw your consent.
- 6) Account Cancellation by Personal Information Subject

Normally, you can deactivate your account by navigating through the steps "My - Account Security - Delete Account." If you are unable to complete the deactivation on your own through the steps mentioned, you can contact us for assistance using the contact information provided at the end of this document. Before deactivating your account, we will verify your personal identity, security status, device information, etc. You acknowledge and understand that account deactivation is an irreversible action. Once your account is deactivated, we will delete or anonymize your related information, except as otherwise required by law or regulation.

You also have the right to object to, or request the restriction of, our use of your Personal Information. If you would like to exercise any of the rights set out in this Section, please contact us using the details set out below. We may refuse to provide access where we have legitimate reasons for doing so under applicable data privacy laws, and in exceptional circumstances may charge a fee for access if the relevant legislation allows us to do so, in which case we will provide reasons for our decision.

After you revoke your consent, we will no longer process the corresponding personal information. However, your decision to withdraw consent will not affect the processing of personal information that was carried out based on your previous authorization.

Responding to Your Requests:

To ensure security, you may need to provide a written request or otherwise verify your identity. We may first require you to authenticate your identity before processing your request. We will respond within [15] working days.

In principle, we do not charge fees for reasonable requests. However, for repeated requests that exceed reasonable limits, we may charge a certain cost fee on a case-by-case basis. We may refuse requests that are baselessly repetitive, require excessive technical means (for example, the need to develop a new system or fundamentally change existing practices), pose risks to the legitimate rights and interests of others, or are extremely unrealistic.

In the following circumstances, in accordance with legal requirements, we will be unable to respond to your request:

- 1) Directly related to national security and defense security;
- 2) Directly related to public security, public health, and major public interests;
- 3) Directly related to criminal investigation, prosecution, trial, and the execution of judgments;
- 4) There is sufficient evidence to indicate that the personal information subject has malicious intent or is abusing their rights;
- 5) Responding to your request would result in serious damage to the legitimate rights and interests of you or other individuals or organizations;
- 6) Involves trade secrets;
- 7) Necessary to safeguard your or another individual's significant legitimate rights and interests, such as life and property, when it is difficult to obtain your consent;
- 8) Responding to your request would result in serious damage to the legitimate rights and interests of you or other individuals or organizations.

17. Feedback, Including Comments, Questions and Complaints

For questions, access/correction/deletion requests, consent-withdrawal requests, complaints or other privacy matters, please contact:

APPEN SINGAPORE PTE. LTD.

Attention: Data Protection Officer / Privacy Contact

Address: 6 Shenton Way, #33-00, OUE Downtown, Singapore 068809

Email: dataprotection@appen.com

If you make a privacy complaint with us, we will respond to let you know how your complaint will be handled. We may ask you for further details, consult with other parties and keep records regarding your complaint when you send us, or provide us with personal information via email (that is, in a message containing a question or comment, or by filling out a form that emails us this information) or via telephone, we use it to respond to your requests.

18. Changes to the Privacy Policy

We may update this Privacy Policy from time to time. Where we make material changes, we will notify you by reasonable means, such as email, in-app notice, pop-up notice or prominent Platform notice. Where required by applicable law, we will obtain your consent to the updated Privacy Policy before continuing the relevant processing. The updated Privacy Policy will take effect from the date stated in the updated version or from the date you accept it, as applicable.

19. General Disclaimers

1) General

Neither we nor any of our affiliates, agents, contractors, employees or other representatives will be liable for losses arising out of or in connection with the use of our Sites to the extent permissible by law. We are only providing our Site and its contents on a “as is” basis and we make no (and expressly disclaim all) representations and/or warranties of any kind, express or implied, with respect to our Sites or its contents including without limitation warranties of merchantability and/or fitness for a particular purpose. In addition, we do not represent or warrant that the information accessible from or via our Sites is accurate, complete or current.

The limitations of liability in relation to our Sites apply to all damages of any kind, including, without limitation, compensatory, direct, indirect or consequential damages, loss of data, loss of opportunity, income, production or profit, loss of or damage to property and claims of third parties. The limitations of liability in relation to our Sites do not limit our liability to the extent that it cannot be limited and/or excluded by applicable law. You are liable for any telephone charges and any charges made by your internet service provider as a result of your use of the internet service.

2) **KYC and Identity Verification**

We may require you to complete KYC and identity verification before you may access certain Platform functions, accept certain tasks or receive payment. KYC and identity verification may be conducted by Didit or another third-party verification provider designated by Appen Singapore. The KYC process may involve the collection of your country/region, identity document type, identity document or passport images, facial images, verification status, verification results and related verification records. Appen Singapore may access or download such information from the verification provider's administrative backend where reasonably necessary for identity verification, fraud prevention, account security, compliance, payment support, dispute handling or legal purposes. If you do not complete required KYC or identity verification, you may not be able to access certain tasks or receive payment.

3) **Payment Processing and Payment Records**

We may collect and use payment-related information to administer and process payments for accepted contributor services. This may include your name, payment provider account details or identifiers, payment status, payment history, monthly revenue statements, task fees, payment error records, currency information and related payment support records. Payments are processed through Payoneer or another payment provider designated by Appen Singapore. The Platform does not provide a wallet, stored value facility, deposit account, withdrawal function or money transfer service. Any monthly revenue statement or payment statement shown on the Platform is an informational record only and does not represent stored monetary value held by Appen Singapore for you.

4) **Access by Appen Affiliates and Service Providers**

Appen Singapore may disclose or make personal data available to Appen affiliates and third-party service providers where reasonably necessary for Platform operation, project management, technical support, issue investigation, troubleshooting, data statistics/analysis, recruitment/project invitation, security, fraud prevention, compliance, KYC, payment processing, hosting, storage, backup, legal, audit or dispute-resolution purposes. Such recipients may include Appen teams located in China, Alibaba Cloud Singapore, Didit, Payoneer and other approved service providers. Access by Appen China teams is intended to be role-based, logged and revocable. Personal data collected through the Singapore Platform will be stored in Singapore, but authorised personnel located outside Singapore may remotely access it for the purposes described in this Privacy Policy.

5) **Data Breach and Security Incident Handling**

If we become aware of a data breach or suspected data breach affecting personal data, we will take reasonable steps to assess, contain, investigate and remediate the incident. Where required

under applicable data protection laws, including the Singapore PDPA, Appen Singapore will notify the relevant authority and/or affected individuals. We may also retain incident records and related information for legal, security, audit, investigation and compliance purposes.