PRIVACY POLICY

Yescan Open Platform
Enterprise API Services

Last Updated: June 3, 2025
Effective Date: June 3, 2025

1. ABOUT Yescan

We, at Nth Power Global Tech Singapore Pte. Ltd ("NTH POWER", "we", "us", "our"), respect your privacy seriously and we are committed to complying with all data protection or privacy laws as are applicable to us. This Privacy Policy ("this Policy") applies to your use of the Yescan Open Platform enterprise API services (collectively, the "Services") provided by NTH POWER, describing how we may collect, use, disclose and otherwise process your personal information when you use our Services.

Our Services provide enterprise-grade document processing capabilities, including but not limited to image scanning and enhancement, Optical Character Recognition (OCR), format conversion and other API interfaces. This Policy applies to all data processed through our API Services.

If you are located in the US or Canada, there are additional jurisdiction-specific supplemental terms that apply to you. Please see the respective sections under "Jurisdiction-Specific Supplemental Terms" below.

Please read this Policy carefully to understand our policies and practices regarding your personal information and how we will protect it. If you do not agree with our policies, do not use our API Services. By using our API Services, you agree to this Policy. Your continued use of our Services after we revise this Policy means you accept those changes, so please check the Policy periodically for updates.

2. DEFINITIONS

"API" (Application Programming Interface)

Refers to the programmatic interfaces we provide that allow your applications to interact with our Services.

"Customer Data"

Refers to all data you submit to our Services for processing through the API, including images, documents and files.

"Processing Results"

Refers to the output data generated by our Services after processing your Customer Data, including recognized text, converted documents and enhanced images.

"Personal Data"

Refers to any information relating to an identified or identifiable natural person, as defined by applicable data protection laws, including the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and other applicable privacy regulations.

"End User"

Refers to any individual whose data may be included in Customer Data submitted to our Services.

3. WHAT INFORMATION WE COLLECT AND HOW WE COLLECT

We collect your personal information in the following ways:

3.1 Information You Actively Provide to Us

When you register to use our API Services, you may provide the following personal information to us:

- Company name and registration information
- Contact name, email address and phone number
- Billing and payment information
- API credentials (API keys, access tokens)

3.2 Customer Data (Data You Submit for Processing)

When you use our APIs, you may submit the following types of data for processing:

- Images and photos of documents
- Scanned documents and PDFs
- Screenshots and digital images

Important: Customer Data may contain personal data of your End Users (such as names, addresses, ID numbers or other personal information visible in documents). You are responsible for ensuring that you have obtained all necessary consents and legal bases for submitting such data to our Services.

3.3 Personal Information We Collect Automatically

To make our Services more useful to you, we may automatically collect the following information, including but not limited to:

- Device information: such as device type, device model, operating system, unique device identification numbers or other identifiers
- Network information: such as IP address, Wi-Fi information, mobile network operator and network status
- Usage information: such as API call logs (timestamps, endpoints called, response codes), usage statistics (call volume, error rates), errors and diagnostic reports

3.4 Personal Information We Receive from Other Sources

We may collect personal information about you from third parties, such as information related to your registration via a third-party account. Information we receive from you will depend on your privacy settings on the applicable third-party platform.

4. DETAILS AND PURPOSES OF PROCESSING

4.1 Helping You Register an Account

In order to create a developer account, you need to provide us with enterprise information such as company name, contact information and email address.

4.2 Providing API Services

Our API Services provide the following categories of document processing capabilities:

(1) Scanning & Image Processing APIs

- B&W Filter - Convert images to black and white format, enhancing document clarity
- Image Enhancement (Enhance) - AI-powered intelligent adjustment of contrast, brightness and sharpness
- Brightening - Intelligently enhance dark details while suppressing overexposure
- Shadow Removal - Remove shadows from document pages
- Watermark Remover - AI-powered intelligent identification and removal of watermarks from documents and images. Important: This feature is intended solely for removing watermarks from documents owned by the user. Users must ensure they hold lawful rights to the relevant documents and shall not use this feature to remove copyright protection watermarks belonging to third parties.
- Grayscale - Convert color documents to grayscale images
- Moire Removal - Eliminate moire patterns caused by digital screen capture
- Ink Saving - Intelligently reduce ink density for optimized printing
- Handwriting Remover - Precisely remove handwritten marks while preserving printed content

(2) OCR (Optical Character Recognition) APIs

- General Document Recognition - High-precision text recognition supporting printed text, handwriting, tables, 20+ languages and formulas
- Table Recognition - Automatic identification of table structures and data with precise row and column restoration
- ID Card Recognition - High-precision extraction of ID card and certificate content

(3) Format Conversion APIs

- Image to Word (pic_to_word) - Convert images to editable Word documents while preserving original layout
- Image to Excel (pic_to_excel) - Convert table images to editable Excel spreadsheets

When you use the above API Services, we will encrypt and transfer the documents and images you submit to our cloud for processing. We promise that your file content will be encrypted for transmission and will not be used for identification or other purposes without your authorization. Once processing is complete, we will automatically delete the relevant Customer Data within 24 hours.

4.3 Customer Data Processing Principles

We process Customer Data only according to the instructions you provide through API requests. We do not use Customer Data for any other purpose, including but not limited to advertising, user profiling or selling to third parties.

4.4 Customer Support

In order to provide customer support service, we may also use your other information, including contact information, inquiries content you submit through our help center or any other feedback channels.

4.5 Other Purposes

In addition to the above purposes, we may also use your information for other purposes necessary to provide the Services, which include: troubleshooting, customizing, improving and developing our services, protecting security and preventing criminal activity, and complying with legal obligations. We use your information only when we have a valid legal basis.

5. COOKIES AND SIMILAR TECHNOLOGIES

Cookies are small text files collecting amounts of data that store on the local drive of your computer or mobile device, which enable your device to be recognized when you visit a website or application.

We, and our affiliates or authorized third-party providers make use of Cookies to provide you with a better, faster and safer user experience. Some Cookies are strictly necessary to make our

Services work and to ensure data and IT security and prevent fraudulent activities. We refer to these as "operationally necessary Cookies". Other Cookies enable us to provide Service functionality, or to enhance user experience on our Services.

Operationally necessary Cookies are strictly necessary to enable access and use of our Services, and you cannot disable them. We may integrate third-party cookies in the future, and you will have the right to decide whether to accept, reject or customize optional Cookies through our Cookie setting tools. If you disable non-operationally necessary Cookies, you can still use our Services although your use of some features and access to some areas on our Services may be limited.

5.1 SDKs and Similar Technologies

Our developer portal may use other technologies that function in a similar way to Cookies, such as Software Developer Kits ("SDKs"):

- For the purpose of log statistics, function configuration, fraud prevention, safety and security, we may integrate SDKs or similar technologies developed by us or by our affiliates, which may collect device information, system information, and network information.
- In order to provide account login and other functions, we may integrate SDKs or APIs provided by third parties.
- To perform basic technical services such as image processing, network parsing, database interaction, etc. more effectively, we utilize a variety of open-source software development kits to collect and process your personal information. However, we do not transfer this personal information to third parties.

6. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

We may disclose, transfer, communicate or otherwise share your personal information to the following parties:

6.1 Our Affiliated Companies

They may use your personal information for purposes such as providing processing services, as described in the Section entitled "Details and Purposes of Processing".

6.2 Third-Party Service Providers

We may, where necessary, share your personal information with third-party service providers, such as cloud service providers, for the purposes outlined in this Policy. These recipients are bound by contract to implement appropriate security measures to protect the personal information they receive and to use it exclusively for the purposes of fulfilling their contractual obligations to us.

6.3 Law Enforcement Agencies, and Government or Regulatory Authorities

We may disclose data when required by applicable law, regulation, legal process or governmental request, or when we believe in good faith that disclosure is necessary to protect our rights, your safety or the safety of others.

6.4 Business Transfers

In the event that we become involved in a transaction with a third party, such as a merger, acquisition, or sale of assets, or if our assets are acquired by a third party in the circumstance that we cease operations or initiate bankruptcy proceedings, it may be necessary to disclose or transfer some or all of our assets, which could include your information, to the acquiring third party as part of such a transaction.

6.5 With Your Consent

We may share data with third parties with your explicit consent.

We do not sell, rent or trade your Customer Data to third parties.

7. DATA RETENTION

We retain your personal information for as long as necessary for the provision of Services. To determine the appropriate retention period, we consider the amount, nature and sensitivity of your personal information, the potential risk of harm from unauthorized use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means and the applicable legal requirements.

The specific information retention periods are determined mainly based on the following criteria (where applicable):

- Customer Data (images/documents submitted for API processing): Automatically deleted within 24 hours after processing is complete
- Account Data: Retained for the duration of the account and for a reasonable period thereafter as required by applicable law
- API Call Logs: Retained for up to 12 months for operational and security purposes
- Billing Records: Retained as required by applicable tax and commercial laws

In cases where we are legally obliged or permitted to keep your personal information longer, we may restrict the processing of your information instead of deleting it (e.g., by restricting access to it, anonymization), as far as legally permissible or required.

8. YOUR RIGHTS

As a user, you may have the right of access, rectification, deletion, restriction of processing and information portability with regard to your personal information, depending upon your jurisdiction and prevailing circumstances.

You can exercise your rights as a data subject by using the contact information provided in Section 12.

The exercise of the above user rights (e.g., withdrawal of consent or erasure) is generally free of charge. However, we may refuse to process (e.g., if the request is manifestly unfounded or excessive) and/or charge an appropriate fee (at most our actual costs) to process your request, in accordance with the applicable laws.

Please note that to protect your information and the integrity of our Services, we may need to verify your identity before processing your request. In some cases we may need to collect additional information to verify your identity, such as your email address.

9. CHILDREN UNDER THE AGE OF 13

Our API Services are designed for enterprise use and are not directed at children under 13 years of age, and we do not knowingly collect or maintain personal information from children under 13. We encourage parents and legal guardians to monitor their children's Internet usage and to help us enforce this Policy.

If we learn we have collected or received personal information from a child under 13 without verification of parental consent, we will delete that information. If you believe we might have any information from or about a child under 13, please contact us at postmaster@Yescanner.com.

10. SECURITY MEASURES

We implement appropriate organizational and technical measures to protect your personal information. For instance, we limit access to your personal information to our employees, agents, contractors and other third parties who require such access to carry out their duties and contractual obligations. We implement both physical access restrictions for our data centers and logical access controls for data and systems access.

In addition, we implement appropriate access control measures to prevent unauthorized access, use, disclosure, modification, disposal or similar risks to the information we hold, and to maintain data accuracy, among other things. We will notify you and the regulatory authorities as required by applicable law, in the event of a data breach incident.

10.1 Technical Measures

- TLS/SSL encryption (HTTPS) for all API communications
- AES-256 encryption for data at rest
- API authentication via secure API keys and access tokens
- Network isolation and firewall protection
- Regular vulnerability assessments and penetration testing
- Automated intrusion detection and prevention systems

10.2 Incident Response

In the event of a data breach affecting your data, we will:

- Notify you without undue delay upon discovery of the breach, and where feasible, within 72 hours of discovery
- Provide details of the nature of the breach, including the categories and approximate number of affected records, likely consequences, and measures taken or proposed to mitigate the impact
- Cooperate with you in fulfilling your obligations to notify supervisory authorities and affected individuals under applicable law

11. INTERNATIONAL TRANSFER OF PERSONAL INFORMATION

We primarily store your personal information in the United States and Singapore. If you are located in Canada, your information is then sent to the United States and Singapore. In this case your personal information is protected by contractual commitments providing adequate protection comparable to Canadian laws.

Your personal information may be transferred to recipients located outside where you reside. The categories of our recipients are as follows:

- Our affiliated companies, who receive the transferred information to help run our Services, to detect, prevent, or otherwise address fraud, misuse of Services, and security or technical issues.
- Third-party service providers, who receive the transferred information to fulfil their contractual obligations, such as cloud computing or other hosting service providers.

We only transfer your personal information outside where you reside where there are appropriate measures put in place in accordance with applicable laws.

For personal data transferred from the EEA, UK or Switzerland, we implement appropriate safeguards to ensure an adequate level of data protection, including:

- Standard Contractual Clauses (SCCs) approved by the European Commission
- Data Processing Agreements with appropriate technical and organizational measures
- Encryption of data in transit and at rest

12. CONTACT US

For any questions, comments regarding this Privacy Policy, or requests to exercise your rights under the laws of your jurisdiction, you may contact our Data Protection Officer via:

Email: postmaster@Yescanner.com

Nth Power Global Tech Singapore Pte. Ltd
51 Bras Basah Road, #03-06 Lazada One,
Singapore 189554

13. SUSPENSION OF OPERATION

If we cease to operate a product and/or service, we will promptly stop collecting your personal information. We will notify you of the cessation of operations one by one or in the form of an announcement, and delete or anonymize the personal information we hold related to the discontinued product and/or service.

14. PRIVACY POLICY UPDATES

We may update this Privacy Policy from time to time as laws and product features change.

When we update our Privacy Policy, we will take appropriate measures to inform you, consistent with the significance of the changes we make and as required by applicable laws. You may receive notifications concerning our major changes to this Privacy Policy timely through various channels, for example, via our developer portal. We recommend you check back frequently to see any updates or changes. Please check the date displayed at the top of the Privacy Policy to see when it was last updated.

15. LEGAL BASIS FOR PROCESSING (GDPR)

For customers and End Users located in the European Economic Area (EEA), United Kingdom (UK) and Switzerland, we process data based on the following legal bases:

- Contract Performance (Article 6(1)(b) GDPR): Processing necessary for the performance of our service agreement with you.
- Legitimate Interests (Article 6(1)(f) GDPR): Processing necessary for our legitimate interests, such as improving services, ensuring security and preventing fraud, provided that such interests do not override your rights.
- Legal Obligation (Article 6(1)(c) GDPR): Processing necessary for compliance with our legal obligations.
- Consent (Article 6(1)(a) GDPR): Where we rely on your consent, you have the right to withdraw consent at any time.

Data Processor Role

For Customer Data containing personal data of your End Users, we act as a Data Processor under the GDPR. You, as the Customer, act as the Data Controller. We process such data only in

accordance with your documented instructions and in accordance with our Data Processing Agreement (DPA), which is available upon request.

16. JURISDICTION-SPECIFIC SUPPLEMENTAL TERMS

16.1 Additional Terms for California Users

Where we are subject to the requirements of the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA), from here on referred to as "CCPA", the following applies:

(1) Collection and Disclosure of California Residents' Personal Information

We explain the categories of data we collect, the sources of that personal information, and the purposes for which we collect and use your personal information in Section 3 "What Information We Collect and How We Collect" and Section 4 "Details and Purposes of Processing". Also, we explain when we may disclose or share your personal information in Section 6 "Disclosure and Sharing of Personal Information".

(2) California Residents' Rights

If you are a California resident and the CCPA does not recognize an exemption that applies to you or your personal information, you have the right to:

- Request us to disclose to you free of charge the following information covering the 12 months preceding your request: the categories of personal information, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information, the categories of third parties to whom the business discloses personal information, and the specific pieces of personal information the business has collected about the consumer.
- Request us to delete the personal information we collected from you unless CCPA recognizes an exemption.
- Request us to correct inaccurate personal information that we maintain about you.
- Request us to limit the use of sensitive personal information if we are using your sensitive personal information beyond what is reasonable and proportionate to provide the requested goods or service. (Please note that we do not collect sensitive information.)
- Be free from unlawful discrimination for exercising your rights including providing a different level or quality of services or denying goods or services to you when you exercise your rights under the CCPA.

(3) Opting Out of "Sales" of Your Personal Information

We don't "sell" any personal information of our users, as those terms are defined under the CCPA. We don't sell or share your personal information for cross-context behavioral advertising.

(4) Additional Information About Disclosures of Personal Information

We may possess de-identified data. De-identified data cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable user, or a device linked to such person. We commit to maintain and use any de-identified data without attempting to re-identify de-identified data.

16.2 Additional Terms for Canada Users

If you are a resident of Canada, you have the following rights regarding your personal information:

- The right to request access to the personal information we hold about you;
- The right to challenge the accuracy and completeness of such information;
- The right to have such information amended as appropriate;
- The right to withdraw your consent of processing.

To exercise any of these rights regarding your personal information or if you have a question or complaint about how we treat your personal information, you may contact our Data Protection Officer via postmaster@Yescanner.com.

17. SUPPLEMENTARY PROVISIONS

17.1 Unless otherwise required by mandatory provisions of applicable local law, this Policy shall be governed by and construed in accordance with the laws of the Republic of Singapore, without regard to principles of conflict of laws.

17.2 For customers located in the EEA, UK or Switzerland, the provisions of this Policy relating to GDPR compliance shall be interpreted in accordance with applicable EU/UK data protection law.

17.3 If any provision of this Policy is found to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

17.4 This Policy, together with the Terms of Service and any applicable Data Processing Agreement (DPA), constitutes the entire agreement between you and us regarding data privacy in connection with the Services.

18. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

For processing activities that are likely to result in a high risk to the rights and freedoms of data subjects (for example, large-scale processing of special categories of personal data such as identity documents through the ID Card Recognition API), we will conduct a Data Protection Impact Assessment (DPIA) in accordance with Article 35 of the GDPR.

Our DPIA process includes:

- Assessing the necessity and proportionality of the data processing activities;
- Identifying and assessing risks to the rights and freedoms of data subjects;
- Developing risk mitigation measures, including security safeguards and protection mechanisms;
- Regularly reviewing and updating the DPIA to ensure its continued effectiveness.

If you need information about DPIAs relevant to your API usage scenario, please contact our Data Protection Officer at postmaster@Yescanner.com.

DATA PROCESSING AGREEMENT

Yescan Open Platform
Enterprise API Services

Last Updated: June 3, 2025
Effective Date: June 3, 2025

1. INTRODUCTION

This Data Processing Agreement ("DPA") is a supplementary agreement between Nth Power Global Tech Singapore Pte. Ltd ("NTH POWER", "we", "us", the "Data Processor") and the customer using the Yescan Open Platform enterprise API services ("you", "Customer", the "Data Controller") regarding the processing of personal data.

This DPA forms an integral part of the Yescan Open Platform Terms of Service (the "Main Agreement") and supplements and further specifies the provisions of the Main Agreement relating to the processing of personal data. In the event of any conflict between this DPA and the Main Agreement, this DPA shall prevail with respect to matters relating to the processing of personal data.

This DPA is intended to ensure that both parties comply with applicable data protection laws when processing personal data, including but not limited to the EU General Data Protection Regulation (GDPR), UK GDPR, the California Consumer Privacy Act (CCPA/CPRA), the Singapore Personal Data Protection Act (PDPA) and other applicable data protection regulations.

2. DEFINITION

Unless otherwise defined in this DPA, terms used herein shall have the meanings assigned to them in the Main Agreement and the Yescan Open Platform Privacy Policy.

"Data Controller"

Means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data, being the Customer (you) under this DPA.

"Data Processor"

Means a natural or legal person which processes personal data on behalf of the Data Controller, being NTH POWER (we/us) under this DPA.

"Sub-Processor"

Means a third party engaged by the Data Processor to carry out specific processing activities on behalf of the Data Controller.

"Personal Data"

Means any information relating to an identified or identifiable natural person ("Data Subject"), as defined by applicable data protection laws.

"Processing"

Means any operation or set of operations performed on personal data, whether or not by automated means, including collection, recording, organization, storage, adaptation, retrieval, use, disclosure, deletion or destruction.

"Data Breach"

Means a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3. SCOPE AND PURPOSE OF PROCESSING

3.1 Purpose of Processing

We process personal data solely for the purpose of providing the API Services under the Main Agreement. Specifically, processing activities are limited to:

- Receiving and processing Customer Data submitted through the API (which may contain personal data of End Users);

- Performing API service functions such as document scanning, image processing, OCR recognition and format conversion;
- Returning processing results;
- Maintaining the security and availability of the API Services.

3.2 Categories of Personal Data Processed

Personal data processed through the API Services may include but is not limited to:

- Personal information contained in Customer Data: names, addresses, ID numbers, contact information and other personal information visible in documents;
- API usage-related data: IP addresses, device information, API call logs.

3.3 Categories of Data Subjects

Data subjects affected by the processing may include:

- Customer's End Users, whose personal data is contained in documents and images submitted to the API Services;
- Customer's employees and authorized representatives.

3.4 Duration of Processing

Data processing continues for the duration of the Main Agreement. Customer Data (images/documents submitted for API processing) is automatically deleted within 24 hours after processing is complete. Account-related data is retained for the period required by applicable law after termination of the Main Agreement and then deleted.

4. DATA PROCESSOR OBLIGATIONS

As the Data Processor, we undertake to:

4.1 Processing on Instructions

Process personal data only on your documented instructions, unless required to do so by applicable law. Where applicable law requires us to process personal data without your instructions, we shall inform you of that legal requirement before processing (unless such law prohibits such notification).

4.2 Confidentiality

Ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. We shall provide appropriate data protection training to all personnel involved in data processing.

4.3 Security Measures

Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing, including but not limited to:

- TLS/SSL encryption (HTTPS) for all API communications;
- AES-256 encryption for data at rest;
- Authentication via secure API keys and access tokens;
- Network isolation and firewall protection;
- Access controls and the principle of least privilege;
- Regular vulnerability assessments and penetration testing;
- Automated intrusion detection and prevention systems;
- Physical security measures for data processing environments.

4.4 Sub-Processors

4.4.1 We shall not engage any Sub-Processor to process personal data without your prior written authorization (including general authorization).

4.4.2 Where you provide general authorization, we shall inform you in writing (including by email) before engaging any new Sub-Processor or replacing an existing one, giving you the opportunity to object to such changes.

4.4.3 Any contract entered into with a Sub-Processor shall contain data protection obligations substantially equivalent to those set out in this DPA.

4.4.4 Current Sub-Processor list:

- Cloud infrastructure service providers (data storage and computing) - Data storage locations: United States and Singapore

4.5 Assistance Obligations

4.5.1 Assist you, to the extent reasonably practicable, in fulfilling your obligation to respond to Data Subject rights requests, including rights of access, rectification, erasure, restriction of processing and data portability.

4.5.2 Assist you, taking into account the nature of processing and the information available to us, in fulfilling your obligations regarding security measures, data breach notification, data protection impact assessments and prior consultation.

4.6 Data Breach Notification

4.6.1 Upon becoming aware of a Data Breach, we shall notify you without undue delay and, where feasible, within 72 hours of discovery.

4.6.2 The notification shall include: a description of the nature of the Data Breach (including the categories and approximate number of Data Subjects affected and the categories and

approximate number of personal data records affected); the name and contact details of the data protection officer or other contact point; a description of the likely consequences of the Data Breach; a description of the measures taken or proposed to remediate the breach.

4.6.3 We shall cooperate with you in fulfilling your obligations to notify supervisory authorities and affected Data Subjects under applicable law.

4.7 Deletion or Return of Data

At the end of the provision of services relating to processing, at your choice, we shall delete or return all personal data and delete existing copies, unless applicable law requires retention of the personal data. Customer Data is automatically deleted within 24 hours after API processing is complete.

4.8 Audit Rights

4.8.1 We shall make available to you all reasonable information necessary to demonstrate compliance with the obligations laid down in this DPA.

4.8.2 Subject to at least 30 days prior written notice and no more than once per year, you or your authorized third-party auditor shall have the right to audit and inspect our compliance with this DPA. Audits shall be conducted during normal business hours and shall not unreasonably interfere with our business operations.

4.8.3 Audit costs shall be borne by you, unless the audit reveals material non-compliance by us, in which case the relevant audit costs shall be borne by us.

5. DATA CONTROLLER OBLIGATIONS

As the Data Controller, you undertake to:

- Ensure that you have a lawful legal basis for collecting and processing personal data submitted through the API Services;
- Provide appropriate privacy notices to your End Users, informing them that their data may be processed through our API Services;
- Obtain necessary consent from End Users for data processing (where applicable);
- Ensure the accuracy and legality of Customer Data submitted to the API Services;
- Promptly respond to Data Subject rights requests and coordinate with us where necessary;
- Comply with all obligations imposed on Data Controllers under applicable data protection laws.

6. INTERNATIONAL DATA TRANSFERS

6.1 Your personal data is primarily stored in the United States and Singapore. When personal data needs to be transferred from the European Economic Area (EEA), the United Kingdom or Switzerland to these locations, we shall implement appropriate safeguards.

6.2 Safeguards for international transfers include:

- Standard Contractual Clauses (SCCs) approved by the European Commission;
- Technical and organizational measures specified in this DPA;
- Encryption of data in transit and at rest;
- Data protection compliance assessments of recipients.

6.3 To enter into Standard Contractual Clauses (SCCs), please contact us at postmaster@Yescanner.com.

7. GDPR-SPECIFIC PROVISIONS

7.1 For processing of personal data subject to the GDPR, this DPA satisfies the requirements of Article 28 of the GDPR for data processor agreements.

7.2 Records of Processing. We shall maintain records of all categories of processing activities carried out on your behalf in accordance with Article 30(2) of the GDPR.

7.3 Data Protection Officer. Our Data Protection Officer can be reached at: postmaster@Yescanner.com.

7.4 Where you are located within the EEA, UK or Switzerland, and applicable law requires the Data Processor to appoint a representative in such territory, we shall designate a representative in accordance with Article 27 of the GDPR and inform you of their details.

8. CCPA-SPECIFIC PROVISIONS

8.1 For purposes of the CCPA, we act as a "Service Provider" processing personal information received from you solely for the business purposes set forth in this DPA and the Main Agreement.

8.2 We shall not:

- "Sell" or "share" (as defined by the CCPA) personal information received from you;
- Retain, use or disclose such personal information outside the business purposes specified in the Main Agreement and this DPA;
- Combine such personal information with personal information collected from other sources, except as permitted by the CCPA for Service Providers.

8.3 We certify that we understand the above restrictions and will comply with them.

9. LIABILITY AND INDEMNIFICATION

9.1 Each party shall be liable for direct losses caused to the other party by its breach of this DPA.

9.2 The limitation of liability provisions in the Main Agreement shall also apply to this DPA, provided that such limitations shall not apply to liability arising from a party's willful or grossly negligent violation of data protection laws.

9.3 Where a regulatory authority imposes a fine on you as a result of our breach of this DPA or applicable data protection laws, and such breach was not caused by our compliance with your instructions, we shall indemnify you for the relevant reasonable costs up to the liability cap specified in the Main Agreement.

10. TERM AND TERMINATION

10.1 This DPA shall take effect on the date you accept the Main Agreement and shall terminate upon the termination or expiration of the Main Agreement.

10.2 Upon termination of this DPA, we shall delete or return all personal data in accordance with Section 4.7.

10.3 Provisions of this DPA that by their nature should survive termination (including but not limited to confidentiality obligations, liability and indemnification provisions) shall survive termination.

11. MISCELLANEOUS

11.1 Unless otherwise provided in this DPA, this DPA shall be governed by and construed in accordance with the laws of Singapore, consistent with the Main Agreement.

11.2 Disputes under this DPA shall be resolved in accordance with the dispute resolution mechanism in the Main Agreement, by submission to the Hong Kong International Arbitration Centre (HKIAC) under its then-applicable arbitration rules.

11.3 If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

11.4 The English version of this DPA shall be the official version. In the event of any conflict or inconsistency between the English version and any other language version, the English version shall prevail.

11.5 Amendments to this DPA require the written agreement of both parties.

12. CONTACT INFORMATION

For any questions about this DPA, please contact us via:

Email: postmaster@Yescanner.com

Nth Power Global Tech Singapore Pte. Ltd
51 Bras Basah Road, #03-06 Lazada One,Nth
Singapore 189554