# Data Processing Agreement

**Version: [v1.0]**

Last Updated: September 3, 2026

This Data Processing Agreement ("DPA") forms part of the Terms of Use or other written agreement between NST LABS TECH LTD, a company incorporated in Hong Kong ("Nstdata", "Processor", "Service Provider", "Contractor", "we", "us", or "our"), and the customer or entity using the Services ("Client", "Controller", "Business", "you", or "your").

This DPA applies where and to the extent Nstdata processes Personal Data on behalf of Client in providing the Services. Nstdata was formerly known as Nstproxy. The operating legal entity is unchanged.

## Definitions

"Agreement" means the Terms of Use, order form, enterprise agreement, or other written agreement governing Client's use of the Services.

"Applicable Data Protection Law" means all privacy, data protection, and data security laws applicable to the processing of Personal Data under this DPA, including where applicable the EU GDPR, UK GDPR, Swiss FADP, Hong Kong Personal Data (Privacy) Ordinance ("PDPO"), and US State Privacy Laws including the CCPA/CPRA.

"CCPA" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act, and its implementing regulations.

"Client Personal Data" means Personal Data processed by Nstdata on behalf of Client under the Agreement.

"EU GDPR" means Regulation (EU) 2016/679.

"Restricted Transfer" means a transfer of Personal Data that requires a lawful transfer mechanism under Applicable Data Protection Law.

"SCCs" means the standard contractual clauses adopted by the European Commission under Commission Implementing Decision (EU) 2021/914, as amended or replaced.

The terms "Personal Data", "Processing", "Controller", "Processor", "Data Subject", "Supervisory Authority", and "Personal Data Breach" have the meanings given in Applicable Data Protection Law.

## Roles of the parties

As between the parties, Client is the Controller or Business of Client Personal Data, or a Processor acting on behalf of a third-party Controller or Business. Nstdata is the Processor, Service Provider, or Contractor processing Client Personal Data on Client's behalf.

Client is responsible for determining the purposes and means of processing, selecting the targets accessed through the Services, establishing a lawful basis, providing required notices, obtaining required consents, complying with target-site terms and third-party rights, and ensuring that its instructions are lawful.

Nstdata may process certain information as an independent controller or business, including account, billing, support, security, fraud prevention, compliance, analytics, marketing, and business operations data, as described in Nstdata's Privacy Policy. This DPA does not apply to that independent processing.

## Scope, instructions, and Client responsibilities

Nstdata will process Client Personal Data only on Client's documented instructions, including the Agreement, this DPA, applicable order forms, product settings, API requests, dashboard configurations, support instructions, and other written instructions accepted by Nstdata, unless required otherwise by law.

If Nstdata believes an instruction violates Applicable Data Protection Law, it will inform Client unless prohibited by law. Nstdata is not responsible for independently determining whether Client's instructions, target selections, collection activities, or downstream uses are lawful.

Client will not submit, collect, or route sensitive Personal Data, children's data, health data, financial account data, government identifiers, biometric data, precise location data, or similarly regulated data through the Services unless expressly permitted by the Agreement and supported by appropriate safeguards.

## Details of processing

The subject matter, duration, nature and purpose of processing, categories of Data Subjects, types of Personal Data, and processing operations are described in Annex 1.

## Confidentiality

Nstdata will ensure that personnel authorized to process Client Personal Data are subject to appropriate confidentiality obligations or statutory duties of confidentiality.

## Security

Nstdata will implement and maintain appropriate technical and organizational measures designed to protect Client Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration, or disclosure, taking into account the nature of the processing and the risks presented.

The current technical and organizational measures are described in Annex 2. Nstdata may update these measures from time to time, provided that the overall level of protection is not materially reduced.

References to ISO 27001, SOC 2, or similar frameworks mean that Nstdata's program is informed by those frameworks unless a formal certification, report, or attestation is expressly provided by Nstdata.

## Subprocessors

Client grants Nstdata general written authorization to engage subprocessors to provide the Services. Nstdata will impose data protection obligations on subprocessors that are substantially similar to those in this DPA and will remain responsible for their performance as required by Applicable Data Protection Law.

Nstdata will make a current list of subprocessors available at [SUBPROCESSOR URL] or on request. Nstdata will provide notice of intended material subprocessor changes at least [30] days before the change where practicable. Client may object on reasonable data protection grounds by notifying Nstdata within the notice period. The parties will work in good faith to resolve the objection. If the objection cannot be resolved, Client may stop using the affected Services or terminate the affected order as its sole remedy.

Nstdata may engage or replace a subprocessor with shorter notice where necessary for security, availability, legal compliance, provider changes, or emergency service continuity.

## Data subject requests

Taking into account the nature of the processing, Nstdata will provide reasonable assistance to Client through appropriate technical and organizational measures, insofar as possible, to help Client respond to Data Subject requests under Applicable Data Protection Law.

If Nstdata receives a request directly from a Data Subject relating to Client Personal Data, Nstdata may direct the Data Subject to Client, unless required otherwise by law.

## Assistance with compliance

Taking into account the nature of processing and information available to Nstdata, Nstdata will provide reasonable assistance to Client with Client's obligations relating to security, Personal Data Breach notification, data protection impact assessments, prior consultation with Supervisory Authorities, and regulator inquiries, where required by Applicable Data Protection Law.

Nstdata may charge reasonable fees for assistance that goes beyond standard product functionality, unless the assistance is required due to Nstdata's breach of this DPA.

## Personal Data Breach

Nstdata will notify Client without undue delay after becoming aware of a Personal Data Breach affecting Client Personal Data. Where practicable, the notice will describe the nature of the breach, categories and approximate number of affected Data Subjects and records, likely consequences, measures taken or proposed, and a contact point for follow-up.

Nstdata's notification of or response to a Personal Data Breach is not an admission of fault or liability. Client is responsible for determining whether notification to Data Subjects, regulators, or others is required, unless Applicable Data Protection Law provides otherwise.

## Deletion or return

Upon termination or expiration of the Services, Nstdata will delete or return Client Personal Data processed on Client's behalf, at Client's choice where required by Applicable Data Protection Law, unless retention is required or permitted by law, the Agreement, legitimate recordkeeping, security, fraud prevention, dispute resolution, tax, accounting, compliance, or backup practices.

Unless otherwise stated in the Agreement, Client is responsible for exporting Client Personal Data before termination. Nstdata may delete Client Personal Data from active systems within [30-90] days after termination and from backups according to standard backup cycles.

## Audits and information

Nstdata will make available information reasonably necessary to demonstrate compliance with this DPA. Where required by Applicable Data Protection Law, Nstdata will allow for and contribute to audits, including inspections, subject to reasonable confidentiality, security, availability, scope, and frequency restrictions.

Audits must be requested with reasonable prior written notice, occur no more than once per year unless required by law or following a confirmed Personal Data Breach affecting Client Personal Data, be conducted during normal business hours, avoid disruption to the Services, and be performed by Client or an independent auditor that is not a competitor of Nstdata.

Nstdata may satisfy audit requests by providing security summaries, policies, questionnaires, certifications, attestations, audit reports, or other documentation where reasonably sufficient.

## International transfers

Client authorizes Nstdata and its subprocessors to process and transfer Client Personal Data in Hong Kong and other jurisdictions where Nstdata or its subprocessors operate, subject to Applicable Data Protection Law.

For Restricted Transfers from the EEA, United Kingdom, or Switzerland to Nstdata in a country without an applicable adequacy decision, the SCCs apply as described in Annex 3. The parties will cooperate to implement supplementary measures where required.

If Nstdata receives a legally binding request from a public authority for access to Client Personal Data, Nstdata will review the request and, where legally permitted and reasonably practicable, notify Client and challenge unlawful or overbroad requests.

## US State Privacy Laws

Where Nstdata processes Personal Data subject to the CCPA or other US State Privacy Laws on behalf of Client, Nstdata will act as a Service Provider, Contractor, or Processor as applicable.

Nstdata will not sell or share Client Personal Data, retain, use, or disclose Client Personal Data outside the direct business relationship with Client, or retain, use, or disclose Client Personal Data for any purpose other than the business purposes described in the Agreement and Annex 1, except as permitted by Applicable Data Protection Law.

Nstdata will not combine Client Personal Data with personal information received from other sources except as permitted by Applicable Data Protection Law. Nstdata will provide the same level of privacy protection required by applicable US State Privacy Laws and will notify Client if it determines that it can no longer meet its obligations.

Client has the right to take reasonable and appropriate steps to help ensure that Nstdata uses Client Personal Data consistently with Client's obligations under applicable US State Privacy Laws. Nstdata will flow down applicable restrictions to subcontractors as required.

## Hong Kong PDPO

Where the Hong Kong PDPO applies, the parties acknowledge that Nstdata may act as a data processor processing personal data on behalf of Client as data user. Nstdata will use contractual, technical, and organizational measures designed to prevent Client Personal Data from being kept longer than necessary for processing and to protect it against unauthorized or accidental access, processing, erasure, loss, or use.

## Order of precedence

If there is a conflict between this DPA and the Agreement, this DPA governs with respect to processing of Client Personal Data on Client's behalf. If there is a conflict between this DPA and the SCCs, the SCCs govern to the extent required for a Restricted Transfer.

## Liability

Each party's liability under this DPA is subject to the limitations and exclusions of liability in the Agreement, except to the extent prohibited by Applicable Data Protection Law or the SCCs.

## Term

This DPA remains in effect for as long as Nstdata processes Client Personal Data on behalf of Client.

## 19. Contact

Questions about this DPA may be sent to:

NST LABS TECH LTD

Email: legal@nstdata.io

Privacy: privacy@nstdata.io

## Annex 1 - Details of processing

**Subject matter:** Provision of the Nstdata Services, including Global Proxy, Crawl, Proxy Manager, APIs, SDKs, dashboard, routing, load balancing, monitoring, support, security, and related functionality.

**Duration:** The term of the Agreement and any period needed for deletion, return, backup expiry, legal retention, dispute resolution, security, billing, or compliance purposes.

**Nature and purpose:** Routing, load balancing, transmission, temporary handling, crawling, rendering, extraction, formatting, delivery, logging, monitoring, troubleshooting, security, abuse prevention, billing support, and operation of the Services.

**Frequency:** Continuous or as initiated by Client through API calls, dashboard actions, configurations, support requests, or other use of the Services.

**Categories of Data Subjects:** As determined by Client, potentially including Client's customers, prospects, employees, contractors, users, website visitors, business contacts, public website publishers, individuals appearing in public web content, and other individuals whose Personal Data is submitted to or processed through the Services by Client.

**Types of Personal Data:** As determined by Client, potentially including names, business contact information, usernames, public profile information, URLs, IP addresses, device and browser information, request metadata, identifiers, content contained in web pages, logs, and other Personal Data submitted to, routed through, collected with, or generated by the Services.

**Sensitive data:** Not intended unless expressly permitted by the Agreement and supported by appropriate safeguards.

**Processing operations:** Collection at Client's instruction, transmission, routing, proxying, crawling, rendering, extraction, transformation, storage where enabled, logging, retrieval, disclosure to Client, deletion, and security monitoring.

## Annex 2 - Technical and organizational measures

Nstdata's technical and organizational measures may include:

- access controls and role-based access to systems;
- authentication and credential management;

- encryption in transit where supported;
- network segmentation and environment separation;
- logging, monitoring, and abuse detection;
- vulnerability management and patching processes;
- incident response procedures;
- personnel confidentiality obligations;
- vendor and subprocessor review;
- backup, restoration, and business continuity measures where applicable;
- data minimization and retention controls where supported by the Services;
- internal policies and training for personnel with access to relevant systems; and
- physical and cloud infrastructure controls provided by hosting and infrastructure providers.

Nstdata may update these measures over time, provided that the overall level of protection is not materially reduced.

## Annex 3 - International transfer terms

For Restricted Transfers subject to the EU GDPR, the SCCs apply as follows:

- Module Two applies where Client is a Controller and Nstdata is a Processor.
- Module Three applies where Client is a Processor and Nstdata is a Subprocessor.
- Clause 9 subprocessor authorization: Option 2, general written authorization, with notice as described in Section 7 of this DPA.
- Annex I, II, and III of the SCCs are completed by Annexes 1, 2, and the subprocessor list referenced in Section 7 of this DPA.

For Restricted Transfers subject to the UK GDPR, the parties will use the UK International Data Transfer Addendum or other lawful mechanism where required.

For Restricted Transfers subject to Swiss data protection law, the SCCs apply with Swiss-specific modifications where required.

## Annex 4 - Subprocessors

A current list of subprocessors is available at [SUBPROCESSOR URL] or on request. The list should identify each subprocessor, processing activity, and relevant processing location.