Version – January 8, 2025

NinjaOne
Data Processing Addendum

NinjaOne, LLC, a Delaware Limited Liability Company located at Suite 200, 3687 Tampa Road, Oldsmar, Florida 34677 ("**NinjaOne**") and the company specified in the signature block ("**Customer**") (each a "**Party**", and collectively, the "**Parties**") have agreed to this Data Processing Addendum.

WHEREAS, NinjaOne operates a SaaS based multi-tenant remote monitoring and management (RMM) platform and provides related technical support for it (collectively, the "**Service**") and provides the Customer with access to it.

WHEREAS, the Parties have entered into one or several agreement(s) and addenda thereto (the "**Agreement**") for the provision of the Service by NinjaOne to the Customer as described in the Agreement.

WHEREAS, in the provision of the Service under the Agreement, NinjaOne may process certain Personal Data on behalf of the Customer, such data being made available by the Customer through the Service directly or indirectly under the Agreement.

NOW, THEREFORE, in consideration of the promises set forth above and the mutual promises, agreements and conditions stated herein, the Parties agree as follows:

Definitions

1. Unless the context requires otherwise, the following definitions apply:

   a. "**Applicable Data Protection Law**" means all applicable laws, regulations and other legal requirements regarding data protection, data security, privacy, or the Processing of Personal Data, as may be amended from time to time. This may include, for example, the Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, "**GDPR**"), together with together with any replacement legislation, similar legislation enacted by the United Kingdom in the course of its transition out of or following its departure from the European Union, or any equivalent legislation of any other applicable jurisdiction, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, the California Consumer Privacy Act and associated regulations ("**CCPA**"), the California Privacy Rights Act and associated regulations ("**CPRA**," and together with the CCPA the "**California Privacy Law**"), as well as U.S. state laws similar to the California Privacy Law, such as the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Act Concerning Personal Data Privacy and Online Monitoring, the Utah Consumer Privacy Act, Texas Data Privacy and Security Act, the Oregon Consumer Privacy Act, Florida Digital Bill of Rights, Montana Consumer Data Privacy Act, the Iowa Consumer Privacy Act, Tennessee Information Protection Act, the Indiana Consumer Data Protection Act, the New Jersey Privacy Act, and the New Hampshire Privacy Act (together the California Privacy Law, as they become effective, the "**U.S. State Privacy Laws**");

   b. "**Connectable Third-Party Service**" means a third-party service that is not provided by NinjaOne or its subprocessors, such as:

      i. Any third-party service purchased from NinjaOne as a reseller or distributor;

      ii. Any third-party service for which Customer holds an active account with the third party, such as:

         A. A third-party service to which Customer connects or integrates with its NinjaOne account via an Application Programming Interface, including, but not limited to, those listed at https://www.ninjaone.com/integrations;

         B. The Google Play Store (which may be accessible through the Service for Customer to manage certain software installations and updates via Customer's own Google account); and

iii. Any third-party content or service that Customer embeds in the Software (such as an embedded video hosted on a third-party service).

c. "**Personal Data**" means any information relating to an identified or identifiable individual, within the meaning of the GDPR (regardless of whether the GDPR applies), and any other information constituting "personal information" as such term is defined in California Privacy Law (regardless of whether California Privacy Law applies);

d. "**Process**" and "**Processing**" mean any operation or set of operations performed on data or on sets of data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

e. "**Schedule**" shall mean a schedule to this DPA, which shall form an integral part of this DPA; and

f. "**Standard Contractual Clauses**" refers to the clauses issued pursuant to the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at http://data.europa.eu/eli/dec_impl/2021/914/oj.

2. The terms used in this DPA not defined herein shall have their meanings given in the Applicable Data Protection Law.

Scope of Applicability of this DPA

3. This DPA shall apply to the Personal Data provided by the Customer to NinjaOne, directly or indirectly, through the Service in connection with the Agreement (the "**Customer Data**").

4. Customer may configure or use the Service to interact with Connectable Third-Party Services and to share or make available Customer Data and other data to such services. NinjaOne is not responsible for Connectable Third-Party Services' Processing of any data, and such Processing is not subject to this DPA.

Processing of Personal Data

5. NinjaOne processes the Customer Data on behalf of the Customer and acts as processor, and the Customer acts as (or on behalf of) controller.

6. As between the Parties, the Customer Data shall remain at all times the Customer's property. An overview of this data and its processing is set forth in Annex B to Schedule 1 of this DPA (regardless of whether the Standard Contractual Clauses apply).

7. Each Party shall fully comply with the obligations that apply to it under the Applicable Data Protection Law.

8. Processing requirements generally:

a. NinjaOne shall treat the Customer Data as confidential information.

b. NinjaOne shall provide at all times during the performance of this DPA sufficient guarantees for its compliance with the requirements of the Applicable Data Protection Law.

c. NinjaOne shall not use, disclose, retain, or otherwise process any Customer Data for purposes other than that which is necessary (i) to provide and support the desired operation of the Services as set forth in the relevant Order Forms, (ii) to the extent permitted by Applicable Data Protection Law, to create aggregated or anonymized data[1] for NinjaOne's lawful use, and (iii) to comply with its obligations under the Agreement, and shall only process the Customer Data in accordance with the Customer's reasonable documented instructions given in this DPA, the Agreement, or Customer's settings within the Service (the "**Permitted Purpose**").

[1] For clarity, data is aggregated or anonymized only if it does not include or constitute Personal Data.

d. If NinjaOne would be required by any applicable legislation to process any Customer Data otherwise than as permitted herein, NinjaOne shall inform the Customer of that legal requirement and the legal basis before processing, unless that law prohibits such information on important grounds of public interest.

e. Without limiting the foregoing obligations of NinjaOne:

   i. NinjaOne shall not "sell" the Personal Data as such term is defined under U.S. State Privacy Laws;

   ii. NinjaOne shall not "share" the Personal Data as such term is defined under California Privacy Law;

   iii. NinjaOne shall not attempt to re-identify any pseudonymized or otherwise de-identified Personal Data received from Customer without Customer's express written permission;

   iv. NinjaOne shall not retain, use, or disclose the Personal Data outside of the direct business relationship between Customer and NinjaOne;

   v. NinjaOne shall comply with any applicable restrictions under Applicable Data Protection Law on combining the Personal Data that NinjaOne receives from, or on behalf of, Customer with Personal Data that NinjaOne receives from, or on behalf of, another person or persons, or that NinjaOne collects from any separate interaction between it and a data subject; and

   vi. For the Personal Data subject to the California Privacy Law, NinjaOne will provide no less than the level of protection required of businesses under the California Privacy Law (in addition to meeting its other obligations in this DPA) and will notify Customer promptly if NinjaOne determines it no longer can provide this level of protection.

f. NinjaOne shall immediately inform the Customer if, in its opinion, an instruction infringes the Applicable Data Protection Law and shall provide details of the actual or potential infringement. NinjaOne shall be entitled to suspend the provisions of any Service that it suspects to infringe the Applicable Data Protection Law until the Customer confirms or amends its instruction in writing. NinjaOne shall be entitled to reject instructions of the Customer that are obviously illegal and/or violate the Applicable Data Protection Law.

g. NinjaOne shall implement appropriate technical and organizational security measures ("**TOM**") set forth in Schedule 2 to this DPA, which meet or exceed relevant industry practice. Those will be applied prior to and during processing of any Customer Data to protect the security, confidentiality and integrity of the Customer Data and to protect the Customer Data against accidental, unlawful or unauthorized processing. This is without prejudice to NinjaOne's right to implement, in its sole discretion, alternatives to the specific measures set forth in Schedule 2 so long as such updates do not lower the overall level of protection. In particular, without limitation, NinjaOne shall protect the Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, use or access to Customer Data transmitted, stored or otherwise processed and against unlawful processing. Such measures shall include, as appropriate:

   i. Processes to protect the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   ii. Processes to restore the availability and access to the Customer Data in timely manner in the event of a physical or technical incident; and

   iii. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for protecting the security of the processing.

h. NinjaOne shall treat Customer Data with confidence and authorize its employees, consultants or agents to access Customer Data only if they require such Customer Data to perform the tasks allotted to them by NinjaOne (the "**Authorized Persons**"). NinjaOne shall require that the Authorized Persons who will process Customer Data:

i. Are aware of and shall comply with the provisions of this DPA;

ii. Are under a duty of confidentiality with respect to the Customer Data no less restrictive than the duties set forth herein prior to any access to the Customer Data. NinjaOne shall ensure that such confidentiality obligations survive the termination of the employment or contracting agreement;

iii. Have received appropriate training in relation to the lawful handling of personal data;

iv. Are subject to user authentication and log-on processes when accessing the Customer Data; and

v. Shall only process the Customer Data as necessary for the Permitted Purpose.

9. Sub-processors.

a. Use of Sub-processors. NinjaOne may engage sub-processors to provide services on its behalf. Such sub-processors may include subsidiaries or affiliates of NinjaOne. Customer hereby consents to engagement of sub-processors by NinjaOne to Process Personal Data under the Agreement subject to the terms set out herein.

b. Obligations. NinjaOne will enter into written contracts with such sub-processors ("**Approved Sub-processor**"), requiring at least a level of data protection and information security as provided for herein, and in any event NinjaOne will remain liable to the Customer for any breach by the Approved Sub-processor that is caused by an act, error or omission of the Approved Sub-processor to the same extent NinjaOne would be liable as if such act, error or omission was NinjaOne's own.

c. Current Sub-processors. The Customer hereby approves the following sub-processors as Approved Sub-processors: https://www.ninjaone.com/approved-subprocessors/ (the "**Approved Sub-processors webpage**"). The Approved Sub-processors reserve the right to retain further subcontractors and to revise their specific security strategy so long as their overall level of security is not lowered.

d. New Sub-processors. NinjaOne shall notify the Customer at least 30 days in advance about its appointment of an Approved Sub-processor, including its identity, where it will process the Personal Data and its relevant data processing activities by (i) updating the Approved Sub-processors webpage (or a different webpage described there) and (ii) sending an email to the Customer on the same day of the update. The Customer shall subscribe to such emails by supplying an email address in the sign-up form available on the Approved Sub-processors webpage.

e. Objections. The Customer shall have the right to object against the use of a sub-processor by providing written notice explaining the basis of the objection to privacyteam@ninjarmm.com within 10 days of NinjaOne's notice of appointment of the sub-processor ("**Objection**"). Customer's failure to provide such Objection within that deadline constitutes its consent to NinjaOne's use of the sub-processor. In case of such Objection, the Parties shall work together in good faith to find a reasonable solution to the Customer's concerns for a period of up to 10 days. If, at the end of such 10-day period, a reasonable solution has not been reached, the Customer may terminate this DPA, along with the Agreement, upon serving 5 days' written notice to NinjaOne. Customer's failure to exercise that termination right within 25 days of NinjaOne's notification to customer under Section 8(d) above shall constitute its consent to NinjaOne's use of the sub-processor.

International Transfers of Personal Data

10. NinjaOne shall not process or transfer any Customer Data outside of the European Economic Area unless an adequate level of protection for international transfers in accordance with the Applicable Data Protection Law of the European Economic Area is ensured (the "**Safeguards**").

11. NinjaOne is a member of the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework (collectively, "**DPF**"). For Customer Data received pursuant to the DPF, NinjaOne shall provide the level of protection required by the DPF and will inform Customer if NinjaOne determines it no longer can do so. To the extent legally required, the Standard

Contractual Clauses shall form part of this DPA and take precedence over the rest of this DPA to the extent of any conflict, and they will be deemed completed as follows:

a. Customer is the exporter and NinjaOne is the importer and a processor. Where Customer acts as a controller with respect to the Personal Data subject to the Standard Contractual Clauses, its Module 2 applies. Where Customer itself acts as a processor with respect to such data, its Module 3 applies.

b. The parties' contact information is set forth in the signature block of this DPA and in Annex 1 to Schedule 1 of this DPA.

c. Clause 7 (the optional docking clause) is included.

d. Under Clause 9 (Use of sub-processors), the parties select Option 2 (General written authorization). The initial list of sub-processors is set forth at https://www.ninjaone.com/approved-subprocessors/, and NinjaOne shall update that list at least 30 days in advance of any intended additions or replacements of sub-processors, as described in Section 8(e) above.

e. Under Clause 11 (Redress), the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body does not apply.

f. Under Clause 17 (Governing law), the parties choose Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The parties select the law of Germany.

g. Under Clause 18 (Choice of forum and jurisdiction), the parties select the courts of Germany.

h. Annexes I and II of the Standard Contractual Clauses are set forth in Schedule 1 of the DPA.

i. By signing this DPA, the parties are signing the Standard Contractual Clauses.

12. With respect to Personal Data for which United Kingdom data protection law governs Customer's transfer to NinjaOne, to the extent legally required, the United Kingdom International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (available as of 21 March 2022 at https://ico.org.uk/for-organisations/guide-to-data- protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer- agreement-and-guidance/) ("**UK SCC Addendum**") forms part of this DPA and shall be deemed completed as follows (with capitalized terms not defined elsewhere having the definition set forth in the UK SCC Addendum):

a. Table 1 of the UK SCC Addendum: The Parties, their details, and their contacts are those set forth in the signature block of this DPA and its Schedule 1.

b. Table 2 of the UK SCC Addendum: the "Approved EU Standard Contractual Clauses" shall be the Standard Contractual Clauses, completed as set forth above.

c. Table 3 of the UK SCC Addendum: the Annexes are set forth in Schedule 1 of this DPA.

d. Table 4 of the UK SCC Addendum: neither party may exercise the termination right set forth in Section 19 of the UK SCC Addendum.

13. With respect to Personal Data for which the Swiss Federal Act on Data Protection ("**Swiss FADP**") governs Customer's transfer to NinjaOne, the EU Standard Contractual Clauses shall be deemed to have the following differences to the extent required by the Swiss FADP:

a. References to the GDPR in the Standard Contractual Clauses are to be understood as references to the Swiss FADP insofar as the data transfers are subject exclusively to the Swiss FADP and not to the GDPR.

b. The term "member state" in the Standard Contractual Clauses shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses.

c. Under Annex I(C) of the Standard Contractual Clauses (Competent supervisory authority):

i. Where the transfer is subject exclusively to the Swiss FADP and not the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

ii. Where the transfer is subject to both the Swiss FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the Swiss FADP, and the supervisory authority is as set forth in the Standard Contractual Clauses insofar as the transfer is governed by the GDPR.

14. Should the Standard Contractual Clauses be revised or replaced, or should a different version of such clauses (or additional clauses) become mandated by any Applicable Data Protection Law, the Parties hereto shall work together in order to implement the new clauses within any applicable legally mandated deadline for doing so.

15. If Customer uses the Service to transfer Personal Data to a third party that is not an Approved Sub-processor, the Customer is responsible for the lawfulness of such transfer.

Duty to Notify and Cooperate

16. NinjaOne shall:

a. promptly give written notice to the Customer if for any reason NinjaOne determines it no longer can comply with any portion of this DPA. In such cases, NinjaOne shall take all reasonable, necessary and appropriate steps to remedy any non-compliance, or cease further processing of Customer Data, and the Customer may immediately terminate the Agreement and this DPA or access to Customer Data, or take any other reasonable action, as determined in its sole discretion;

b. cooperate with the Customer to assist the Customer in complying with its obligations with regard to the security of the processing of Customer Data, taking into account the nature of the processing and the information available to NinjaOne;

c. promptly give written notice to the Customer after becoming aware of any accidental or unlawful destruction, loss, alteration, disclosure or other Processing of, or access to, Personal Data ("**Data Breach**"). In such case, NinjaOne shall promptly inform the Customer of the Data Breach without undue delay and shall provide all such information and cooperation as the Customer may reasonably request for the Customer to fulfill its data breach reporting obligations under Applicable Data Protection Law. The notice must include NinjaOne's assessment of the following: (i) the nature of the Data Breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned; (ii) the likely consequences of the Data Breach; and (iii) measures taken or proposed to be taken by NinjaOne to address the Data Breach, including, where applicable, measures to remedy or mitigate its possible adverse effects. NinjaOne shall take reasonable measures and actions to remedy or mitigate the effects of the Data Breach, taking into account the circumstances of the Data Breach, and shall keep the Customer up-to-date about developments in connection with the Data Breach;

d. cooperate with the Customer in the preparation of any data protection impact assessments performed by the Customer, whether on a mandatory or voluntary basis. NinjaOne shall provide the Customer with all such reasonable and timely assistance as the Customer may require in order to conduct a data protection impact assessment in relation to the Customer Data and, if necessary, to consult with its relevant data protection authority. NinjaOne agrees and acknowledges that if the Customer receives a request from a data protection authority, the Customer may share with such authority the terms of this DPA, the Agreement and any other information NinjaOne provides as reasonably necessary to demonstrate compliance with this DPA or Applicable Data Protection Law;

e. provide any reasonable cooperation requested by the Customer to enable it to respond and comply with (i) the exercise of rights of data subjects pursuant to Applicable Data Protection Law (such as their right of access, right to rectification, right to object to the processing of their Personal Data, right to erasure and their right to restriction of processing of their Personal Data and their right to data portability) and (ii) any other correspondence, enquiry or complaint received from a data subject, regulatory authority or any other third party in respect of Customer Data processed by NinjaOne under this DPA. NinjaOne shall promptly inform the Customer of any requests relating to the exercise of such rights or complaints, enquiry or correspondence if they are received directly by NinjaOne and

shall provide all details thereof, and Customer shall lawfully handle such requests. Furthermore, NinjaOne shall provide all Customer Data requested by the Customer, within a reasonable timescale specified by the Customer and shall provide such assistance to the Customer to comply with the relevant request within the applicable timeframes.

f. upon the Customer's reasonable request, make all such records, appropriate personnel, data processing facilities and any relevant materials available relating to the processing of the Customer Data available to the Customer in order to allow the NinjaOne to demonstrate compliance with this DPA. The Customer shall take all reasonable measures to prevent unnecessary disruption to NinjaOne's operations. The Customer will not exercise its inspection rights as set forth in this clause more than once in any twelve (12) calendar month period and with ninety (90) days' prior written notice, except (i) if and when required by instruction of a competent data protection authority or (ii) the Customer believes a further audit is necessary due to a data breach suffered by NinjaOne. The Customer shall bear the costs of such inspections. The Customer will treat the results of the inspections as confidential and share them with NinjaOne in a timely manner.

17. Customer has the right to take reasonable and appropriate steps to (i) ensure that NinjaOne is using Customer Data consistent with Customer's obligations under Applicable Law and (ii) stop and remediate unauthorized use of Personal Data.

Effect of Termination

18. Within ninety (90) days following the expiration or termination of the Agreement, NinjaOne shall delete or return all Customer Data and any existing copies thereof in its possession, at NinjaOne's sole expense, unless any applicable law requires the further storage of the Customer Data. At the Customer's request, NinjaOne shall certify to the Customer that all Customer Data has been deleted in accordance with the foregoing. If NinjaOne cannot delete the Customer Data due to technical reasons, NinjaOne will immediately inform the Customer and will take all appropriate steps to:

a. Come as close as practicable to a complete and permanent deletion of the Customer Data; and

b. Make the remaining Customer Data which is not deleted or effectively anonymized unavailable for any further processing except to the extent required by applicable law.

General Terms

19. Once executed by each party, this DPA (including, to the full extent applicable, the EU Standard Contractual Clauses, supplemented as described in the DPA for the United Kingdom and Switzerland) forms part of the Agreement. To the full extent they are applicable, the EU Standard Contractual Clauses take precedence over the rest of the DPA to the extent of any conflict, and the DPA takes precedence over the rest of the Agreement to the extent of any conflict

20. To the maximum extent allowed by applicable law, the limitations of liability and any exclusions of damages set forth in the Agreement govern the aggregate liability for all Customer claims arising out of or related to this DPA and/or the Agreement against NinjaOne. These limitations of liability and exclusions of damages apply to all claims, whether arising under contract, tort, or any other theory of liability.

21. IN WITNESS WHEREOF, the Parties hereto have executed this DPA through their authorized representatives.

NINJAONE, LLC	**CUSTOMER'S COMPANY NAME:**
BY: DocuSigned by: Brian Krupczak B12C09F15DB4479...	_____
NAME: Brian Krupczak	BY: _____
TITLE: Asst. General Counsel	NAME: _____
DATE: 1/8/2025	TITLE: _____
	DATE: _____
	REGISTERED OFFICE ADDRESS:
	Contact person's name and title (if different from signatory):
	Contact person's contact details (if different from email address of Customer's main administrative account in the NinjaOne platform):
	Customer's role under Standard Contractual Clauses, to the extent applicable, is controller unless this box is ticked for processor: [ ]
	If applicable, identity and contact details of Customer's data protection officer and/or representative in the European Union (if applicable):

Schedule 1: Annexes of the Standard Contractual Clauses

ANNEX I

A. LIST OF PARTIES

Data exporter	
Name	As set forth in the DPA signature block above.
Address	As set forth in the DPA signature block above.
Contact person's name, position, and contact details	As set forth in the DPA signature block above.
Data protection officer	As set forth in the DPA signature block above.
Activities relevant to the data transfer	Use of the importer's Services
Role	As set forth in the DPA signature block above.
Signature and date:	Located in the DPA signature block above.

Data importer	
Name	NinjaOne, LLC
Address	Suite 200, 3687 Tampa Road Oldsmar, Florida 34677
Contact person's name, position, and contact details	Chief Trust Officer privacyteam@ninjaone.com
Data protection officer	dpo@ninjaone.com
Activities relevant to the data transfer	Provision of the Service to the data exporter
Role	Processor
Signature and date:	Located in the DPA signature block above.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
May include end users or employees and members of the staff of the Customer or its customers.

Categories of personal data transferred
All Customer Data that is subject to the DPA, consisting mainly of the following, to the extent it is Personal Data:

- IP address(es) for end-user equipment/devices managed by the Service belonging to the Customer and/or their clients: e.g., laptops, desktops.
- System names for end-user equipment/devices managed by the Service belonging to the Customer and/or their clients: e.g., laptops, desktops.
- Hardware/Software details (including performance and utilization metrics) of end-user equipment/devices managed by the Service belonging to the Customer and/or their clients: e.g., laptops, desktops.
- Usernames stored on end points managed by the Service or used to access the NinjaOne management console belonging to the Customer and/or their clients.
- Personal Data in the names of files or folder structures that the Customer managed by the Service.
- Personal Data in files that Customer transmits or receives through the Service.
- Personal Data in files or other data or content that Customer backs-up through the Service, but only to the extent that Customer uses the NinjaOne Backup product to do so.
- Browser/cookie details of end-user equipment/devices managed by the Service belonging to the Customer and/or their clients: e.g., laptops, desktops (for avoidance of doubt, excluding those processed by any Connectable Third-Party Service).
- System logs of end-user equipment/devices managed by the Service belonging to the Customer and/or their clients: e.g., laptops, desktops.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
None

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
Continuous

Nature of the processing
Collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure and destruction to provide the Service to the Customer.

Purpose(s) of the data transfer and further processing
As set forth in Section 7 of the DPA.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
For the term of the Agreement and (if applicable) to support a subsequent return of Data to the Customer, unless a legal obligation requires longer retention.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
As set forth above.

C. COMPETENT SUPERVISORY AUTHORITY

Determined under Clause 13 of the Standard Contractual Clauses. To the extent legally permissible, it is the Berlin Commissioner for Data Protection & Freedom of Information.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

See Schedule 2 below.

Schedule 2: Security Safeguards

NinjaOne will adopt and maintain appropriate security measures, including organizational and technical controls, to protect Customer Data and NinjaOne systems and devices used to process or access Customer Data ("**Systems**"), against unauthorized, accidental or unlawful access, loss, alteration, modification, disclosure, collection, copying, destruction or processing. The specific measures include the following or updates to these measures that do not lower the level of protection provided by these measures:

1. **Physical Controls**

   1.1. **General.** NinjaOne shall maintain procedures for the physical protection of Systems and Customer Data, including information, software, and hardware.

   1.2. **Access restrictions.** NinjaOne will maintain physical access control mechanisms (such as locks and/or guards) at NinjaOne facilities. NinjaOne uses the AWS Cloud Platform infrastructure, which provides physical access controls.

2. **Security Monitoring**

   2.1. **Generally.** NinjaOne shall maintain procedures to determine whether any compromise of Systems or Customer Data (e.g. loss or modification of information, software or hardware) has occurred.

   2.2. **Logging.** Local logging must be enabled on all Systems to capture useful information such as date, timestamp, and (depending on the System) event source, user, source addresses, and destination addresses.

   2.3. **Monitoring.** NinjaOne must analyze Systems for anomalous and suspicious activity to assist in the identification of possible security incidents.

3. **Personnel**

   3.1. **Confidentiality.** NinjaOne must ensure that all NinjaOne personnel with access to Customer Data or Systems have signed a confidentiality agreement requiring them to keep Customer Data confidential and prohibiting them from copying or disclosing Customer Data without prior authorization.

   3.2. **Policy Agreement.** All NinjaOne employees must read and acknowledge NinjaOne's Code of Conduct, Acceptable Use Policy, and Employee Handbook. All NinjaOne personnel with access to Customer Systems must comply with Customer employee security procedures regarding such Systems. Customer shall provide such procedures to applicable NinjaOne personnel or to NinjaOne for distribution to them.

   3.3. **Background Checks.** NinjaOne must perform commercially reasonable background checks on any NinjaOne employees in the United States who will have access to Customer Data or Systems.

   3.4. **Reporting.** NinjaOne shall maintain a clear reporting structure for NinjaOne personnel to communicate security issues and establish a clear reporting format for any incident or security policy violation.

4. **Integrity and Availability.** NinjaOne must maintain controls for the integrity and availability of Customer Data and Systems.

5. **Training and Awareness**

   5.1. **Training.** NinjaOne shall provide training to NinjaOne users and administrators with access to Systems and Customer Data that covers appropriate role-based topics in methods, procedures, and security.

   5.2. **Security Awareness.** NinjaOne shall ensure that NinjaOne personnel with access to Systems and Customer Data are aware of their security responsibilities and shall require annual awareness training for such personnel.

6. **Change Management.** NinjaOne shall maintain documented processes for change management.

7. **Access Controls.** NinjaOne shall:

   7.1. Provide NinjaOne personnel with access to Customer Data and Systems only if they require such access to perform the services described in the Agreement, or to facilitate the performance of such services, such as system administrators, consistent with the concepts of least privilege and need-to-know.

   7.2. Promptly terminate access privileges to Customer Data and Systems for any NinjaOne personnel who no longer need such access and conduct reviews of access lists to confirm that access privileges have been appropriately provisioned and terminated no less than quarterly.

7.3. Maintain an authorization process for user access and privileges that requires that access requests be approved by a different individual than the requester, consistent with the concept of segregation of duties.

7.4. Maintain a list or log of individuals authorized to access Systems and Customer Data, and what their rights and privileges are with respect to such access.

7.5. Enforce complex password requirements and multifactor authentication on all Systems.

8. **Vulnerability management.** NinjaOne shall:

8.1. Perform (1) automated quarterly vulnerability scans and (2) periodic authenticated vulnerability scanning on all Systems to identify potential vulnerabilities on such Systems.

8.2. Remediate identified vulnerabilities in a timely, risk-based manner, including timely implementation of manufacturer- and developer-recommended security updates and patches to operating systems and third-party software storing, processing, or transmitting Customer Data, or otherwise installed on NinjaOne Systems.

9. **Penetration testing.** NinjaOne shall perform, or engage a qualified third party to perform, an annual penetration test on all NinjaOne Systems that process Customer Data.

10. **Antivirus.** Antivirus and malware protection software with up-to-date definitions and signatures must be maintained and enabled on all NinjaOne Systems.

11. **Network security.** NinjaOne shall maintain reasonable network security measures, including but not limited to firewalls to segregate NinjaOne's internal networks from the internet, risk-based network segmentation, and intrusion prevention or detection systems to alert NinjaOne to suspicious network activity.

12. **Encryption.** All Customer Data must be encrypted in transit and at rest using industry-standard encryption algorithms, and in accordance with industry standards for secure key and protocol negotiation and key management.

13. **Code and application security.** To the extent that NinjaOne develops custom code or applications on Customer's behalf, NinjaOne shall perform security testing against (i) the vulnerabilities described in the version of the OWASP Top Ten List available as of the Effective Date, (ii) any vulnerabilities described in changes to the OWASP Top Ten List after the Effective Date (within a reasonable time after such changes are initially published), (iii) any other vulnerabilities NinjaOne identifies through industry standard testing, or (iv) vulnerabilities reported to NinjaOne by any third party. The term "OWASP Top Ten List" shall mean the Open Web Application Security Project's Top Ten list (available at https://owasp.org/www-project-top-ten/ or an updated website).

14. **Audit and Monitoring.**

14.1. **ISO27001 / SOC 2 Type II Attestation.** During the term of the Agreement, NinjaOne must maintain a current ISO27001 and/or SOC 2 Type II attestation covering at minimum the environment in which Customer Data is stored. NinjaOne must furnish a copy of its attestation to Customer annually upon request at renewal.

14.2. **Audit.** During the term of the Agreement, Customer may audit NinjaOne's compliance with this Schedule 2 as set forth in Section 15(f) of the DPA.

14.3. **Documentation.** Customer reserves the right to request documentation to verify NinjaOne's compliance with this Addendum as set forth in the DPA.