DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is executed as of the Effective Date as set out in Section 2 below ("**Effective Date**") by 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**").

WHEREAS, NinjaOne operates a SaaS based multi-tenant 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:

1. Definitions

Unless the context requires otherwise, the following terms shall have the meaning set out in this Section 1:

"**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**"), and similar U.S. state laws;

"**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)

"**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.

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

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

2. Formation of this DPA

This DPA comes into effect on the "Effective Date," which shall be the date on which this DPA is signed by the Customer.

3. Scope of Applicability of this DPA

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 as described in Schedule 1 to this DPA (the "**Customer Data**"). Customer may choose to configure or use the Service to share Customer Data and other data with third-party services ("**Connectable Third-Party Services**"), some of which may be purchased from NinjaOne as a reseller or distributor. NinjaOne is not responsible for Connectable Third-Party Services' Processing of any data, and such Processing is not subject to this DPA.

4. Processing of Personal Data

4.1 NinjaOne processes the Customer Data on behalf of the Customer and acts as processor and the Customer acts as controller.

4.2 Each Party shall fully comply with the obligations that apply to it under the Applicable Data Protection Law. It is expressly agreed upon between the Parties that the Customer Data shall remain at all times the Customer's property.

4.3 In its capacity as processor:

(a) NinjaOne shall treat the Customer Data as confidential information and process the Customer Data solely and exclusively for the purpose of providing the Service to the Customer and on Customer's behalf.

(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. NinjaOne shall not use, disclose, retain, or otherwise process any Customer Data for purposes other than that which is strictly necessary for the performance of its obligations under the Agreement, and shall only process the Customer Data in accordance with the Customer's documented instructions (the "**Permitted Purpose**") given in this DPA, the Agreement or by

any other means during the performance of this DPA. 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 before processing, unless that law prohibits such information on important grounds of public interest. Without limiting the foregoing obligations of NinjaOne:

i. NinjaOne shall not "sell" the Personal Data as such term is defined under California Privacy Law and similar U.S. state laws;
ii. NinjaOne shall not "share" the Personal Data as such term is defined under the California Privacy Rights Act ("CPRA") and related regulations;
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 CPRA, NinjaOne will provide no less than the level of protection required under the CPRA (in addition to meeting its other obligations in this DPA).

(c) NinjaOne shall immediately inform the Customer if, in its opinion, an instruction infringes the Applicable Data Protection Law and shall provide details of the breach or potential breach. 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.

(d) NinjaOne shall implement appropriate technical and organizational security measures 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. 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. NinjaOne shall ensure a level of security appropriate to the risks presented by the processing of Customer Data and the nature of such Customer Data. 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;
iii. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for protecting the security of the processing; and

iv. A process for deleting, forgetting, amending, correcting or porting the Customer Data as instructed by the Customer.

At a minimum, such measures shall include the organizational and technical measures ("**TOM**"), which meet or exceed relevant industry practice. These measures (or alternatives that NinjaOne may implement in its sole discretion that do not lower the overall level of protection) shall remain in place throughout the duration that NinjaOne provides the Service to the Customer or until NinjaOne ceases to process Customer Data (whichever is later);

(d) 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 ensure that the Authorized Persons who will process Customer Data:

vii. Are aware of and shall comply with the provisions of this DPA;
viii. 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;
ix. Have received appropriate training in relation to the Applicable Data Protection Law;
x. Are subject to user authentication and log-on processes when accessing the Customer Data; and
xi. Shall only process the Customer Data as necessary for the Permitted Purpose.

(e) NinjaOne shall immediately inform the Customer if Customer Data is seized or confiscated or at risk due to insolvency or other proceedings or measures of third parties, unless NinjaOne is prohibited to do so by court or by order of the competent authority. NinjaOne shall inform the competent authorities that the usage of the Customer Data is at the sole discretion of the Customer.

4.4 Sub-processors.

(a) Use of Sub-processors. NinjaOne may engage sub-processors from time to time 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**"), guaranteeing 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 the 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, if the Customer subscribes 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 30 days. If, at the end of such 30-day period, a reasonable solution has not been reached, the Customer may terminate this DPA, along with the Agreement, upon serving 10 days' written notice to NinjaOne.

5. International Transfers of Personal Data

NinjaOne or any Approved Sub-processor shall not process or transfer any Customer Data (nor permit the Customer Data to be transferred) outside of the European Economic Area unless an adequate level of protection in accordance with the Applicable Data Protection Law is ensured (the "**Safeguards**").

NinjaOne holds an AICPA Service Organization Control (SOC 2) Type II certification. Our annual SOC 2 examination reviews 144 out of 150 individual controls that overlap with the ISO 27001 standard. NinjaOne also protects Personal Data through compliance and security controls based on the following frameworks and guidelines (on a non-certification basis):

- NIST Cyber Security Framework Revision 1.1
- U.S. Department of Defense DFARS 252.204-712
- NIST Special Publication 800-171 Revision 2
- NIST Special Publication 800-53 Revision 5
- United States Cybersecurity Maturity Model Certification (CMMC) Level 3

To the extent such should become necessary, other Safeguards will be enacted and may include, without limitation: (1) a transfer only to countries which ensure an adequate level of data protection according to an adequacy decision of the European Commission, or (2) or an alternative recognized compliance standard for the lawful transfer of Personal Data - as defined in the GDPR - outside the European Economic Area, such as EU Standard Contractual Clauses.

In order to legitimize that transfer of Customer Data, which are subject to this DPA from the Customer to NinjaOne, the Parties hereby enter into the EU Standard Contractual Clauses

which are attached hereto as Schedule 3 and apply to the extent legally required. Should the current EU Standard Contractual Clauses be replaced by further clauses, the Parties hereto shall work together in order to implement the revised clauses.

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):

- Table 1 of the UK SCC Addendum: The Parties, their details, and their contacts are those set forth in Schedule A.
- Table 2 of the UK SCC Addendum: the "Approved EU Standard Contractual Clauses" shall be the EU Standard Contractual Clauses set forth in Schedule 3 of this DPA.
- Table 3 of the UK SCC Addendum: the Annexes are set forth at the conclusion of the EU Standard Contractual Clauses set forth in Schedule 3 of this DPA.
- Table 4 of the UK SCC Addendum: neither party may exercise the termination right set forth in Section 19 of the UK SCC Addendum.

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:

- References to the GDPR in the EU 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.
- The term "member state" in the EU 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 EU Standard Contractual Clauses.
- References to personal data in the EU Standard Contractual Clauses also refer to data about identifiable legal entities until the entry into force of revisions to the Swiss FADP that eliminate this broader scope.
- Under Annex I(C) of the EU Standard Contractual Clauses (Competent supervisory authority):
  - 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.
  - 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 EU Standard Contractual Clauses insofar as the transfer is governed by the GDPR.

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.

6. Duty to Notify and Cooperate

NinjaOne shall promptly give written notice to and/or shall fully cooperate with the Customer:

(a) if for any reason (i) NinjaOne cannot comply, or has not complied, with any portion of this DPA, (ii) it would be in breach of or has breached any Applicable Data Protection Law governing its processing of Customer Data, or (iii) Applicable Data Protection Law no longer allows the lawful transfer of Customer Data from the Customer to NinjaOne. 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) to enable the Customer to comply 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) upon becoming aware of any data breach. In such case, NinjaOne shall promptly inform the Customer of the data breach without undue delay and shall provide all such timely information and cooperation as the Customer may reasonably require including in order for the Customer to fulfill its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. NinjaOne shall further take such reasonable measures and actions as are necessary to remedy or mitigate the effects of the data breach and shall keep the Customer up-to-date about developments in connection with the data breach;

(d) 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 the terms of this DPA, the Agreement and any other information NinjaOne provides to demonstrate compliance with this DPA or Applicable Data Protection Law.

In addition to the foregoing, if NinjaOne believes or becomes aware that its processing of the Customer Data is likely to result in a high risk (as defined in the Applicable Data Protection Law, relevant regulatory guidance and case law) with regard to the data protection rights and freedoms of data subjects, it shall promptly inform the Customer.

(e) to 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. 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. NinjaOne understands that any response to such direct requests requires prior written authorization from the Customer. If necessary, NinjaOne shall co-operate with the competent supervisory authority;

(f) upon the Customer's reasonable request, to 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 Customer to demonstrate compliance with its obligations laid down in the Applicable Data Protection Law. 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 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. Customer has the right to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data.

NinjaOne hereby certifies that it understands its obligations under this DPA and that it will comply with them.

7. Effect of Termination

Within ninety (90) days following the expiration or termination of the Agreement, NinjaOne shall delete 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:

i. Come to the closest possible to a complete and permanent deletion of the Customer Data and to fully and effectively anonymize the remaining Customer Data; and
ii. Make the remaining Customer Data which is not deleted or effectively anonymized unavailable for any further processing except to the extent required by any applicable law.

8. Order of Precedence

Upon Customer's execution, this DPA (including the EU Standard Contractual Clauses, supplemented as described in the DPA for the United Kingdom and Switzerland) forms part of the Agreement. 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.

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

NINJAONE, LLC	**CUSTOMER'S COMPANY NAME:**
DocuSigned by: Brian Krupczak B12C09F15DB4479...	
BY:	BY:
NAME: Brian Krupczak	NAME:
TITLE: Asst. General Counsel	TITLE:
DATE: 3/14/2023	DATE:
	REGISTERED OFFICE ADDRESS:

ninjaOne

Schedule 1: Data Processing Schedule

1. Categories of Data

The Customer Data processed by NinjaOne shall include the following data (provided that the provisions of the DPA shall only apply if and to the extent such data constitute Personal Data):

- IP address(es) for end-user equipment/devices belonging to the NinjaOne Customer and/or their clients: e.g., laptops, desktops
- System names for end-user equipment/devices belonging to the NinjaOne Customer and/or their clients: e.g., laptops, desktops
- Hardware details of end-user equipment/devices belonging to the NinjaOne Customer and/or their clients: e.g., laptops, desktops
- Software details of end-user equipment/devices belonging to the NinjaOne Customer and/or their clients: e.g., laptops, desktops
- Usernames belonging to the NinjaOne Customer and/or their clients
- Personal Data in the names of files or folder structures that the Customer manages using the Service;
- Personal Data in files that Customer transmits or receives through the Service;
- Browser/user-agent details of end-user equipment/devices belonging to the NinjaOne Customer and/or their clients: e.g., laptops, desktops
- Performance and utilization metrics of end-user equipment/devices belonging to the NinjaOne Customer and/or their clients: e.g., laptops, desktops
- Error codes of end-user equipment/devices belonging to the NinjaOne Customer and/or their clients: e.g., laptops, desktops

2. Categories of data subjects

Data subjects are the persons whose Data is processed by the NinjaOne and may include end users or employees and members of the staff of the Customer and/or their clients.

3. Permitted processing operations for NinjaOne

The processing consists of all data processing activities that are performed following the instructions of the Customer and that are necessary to deliver the Service to the Customer and for the purposes set out in the Agreement.

4. Permitted Purposes

NinjaOne may process Data in accordance with the purposes set out in the Agreement and the DPA.

5. Duration

The duration of the processing is limited to the duration needed to perform its obligations under the Agreement, unless a legal obligation applies. The obligations of NinjaOne with regard to

the Data processing shall in any case continue until the Data have been properly deleted or have been returned at the request of the Customer.

ninjaOne

Schedule 2: Organizational and technical measures (TOM)

The organizational and technical measures in relation to data privacy, include, but are not limited to:

- Review and audit vendors regarding data privacy standards.
- Provide audited physical, virtual and organizational access control.
- Audit of employee data access behavior.
- Protect data via physical and virtual security systems.
- Processes to regularly test, assess and evaluate effectiveness of TOMs.
- Anonymize data in certain processes where no Personal Data is needed.
- Encryption of certain data streams with FIPS 140-2 compliant cryptographic models.
- Annual examinations and testing of compliance and security controls through the AICPA Service Organization Control (SOC 2) process of testing Trust Service Principles. The AICPA SOC 2 examination includes 144 [out of 150] individual controls that overlap with the ISO27001 standard.
- Compliance and security controls that are based upon the following frameworks and guidelines (on a non-certification basis):
    - NIST Cyber Security Framework Revision 1.1
    - U.S. Department of Defense DFARS 252.204-712
    - NIST Special Publication 800-171 Revision 2
    - NIST Special Publication 800-53 Revision 5
    - United States Cybersecurity Maturity Model Certification (CMMC) Level 3

ninjaOne

STANDARD CONTRACTUAL CLAUSES
Module Two: Transfer controller to processor

SECTION I

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:
  (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
  (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 - Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
  (iii) Clause 9(a), (c), (d) and (e);
  (iv) Clause 12(a), (d) and (f);
  (v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7
Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope,

context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[1] (in the same country as the data importer or in another

[1] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated

third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least four weeks in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights

---

into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

for data subjects.[2] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

[2] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[3];

[3] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall

---

experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Germany.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ninjaOne

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s)	
Name	
Address	
Contact person's name, position, and contact details	
Data protection officer	
Activities relevant to the data transfer	
Role	Controller

Date _____ Signature _____

Data importer(s)	
Name	NinjaOne, LLC
Address	Suite 200, 3687 Tampa Road, Oldsmar, Florida, 34677
Contact person's name, position, and contact details	Mike Arrowsmith Chief Trust Office privacyteam@ninjaone.com
Data protection officer	Mike Arrowsmith
Activities relevant to the data transfer	The data importer provides the Service to the data exporter in accordance with the Agreement.
Role	Processor

3/14/2023

Date _____

DocuSigned by:
Brian Krupczak
B12C09F15DB4479...

Signature _____

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred	Data subjects are the persons whose data is processed by the data Processor and may include end users or employees and members of the staff of the Controller.
Categories of personal data transferred	Personal data provided by the Controller to Processor, directly or indirectly, through the use of NinjaOne's SaaS based multi-tenant RMM platform and technical support services (collectively, the "Service"), consisting mainly of the following, to the extent is personal data: IP addresses and other technical details regarding end-user devices; filenames; folder names; and the arbitrary content of any files that Controller may transmit through the Service
Sensitive data transferred (if applicable) and applied restrictions or safeguards	n/a
Frequency of the transfer	Continually
Nature of the processing	The nature of the processing is the processing of data to provide its Service to the Controller.
Purpose(s) of the data transfer and further processing	The Processor may process Data only to provide the Service.
Period for which the personal data will be retained or criteria used to determine that period	The duration of the processing is limited to the duration needed to perform its obligations under the Agreement, unless a legal obligation applies. The obligations of the Processor with regard to the Data processing shall in any case continue until the Data have been properly deleted or have been returned at the request of the Controller.
For transfers to (sub-) processors: subject matter, nature and duration of the processing	As set forth above.

ninjaOne

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.

Measures of pseudonymisation and encryption of personal data	• NIST SP # 800-35, Guide to Information Technology Security Services
	• NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems
	• NIST SP # 800-95, Guide to Secure Web Services
	• NIST SP # 800-123, Guide to General Server Security
	• NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing
	• NIST SP # 800-160, Systems Security Engineering
	• For any and all data transferred between the NinjaOne Agent and the NinjaOne platform, FIPS 140-2 compliant cryptographic modules enforced via TLS encryption.
	  ○ Specifically, all ciphers are Perfect-Forward Secrecy (PFS), with the following cryptography:
	  ▪ ECDHE RSA with AES128-GCM and SHA256
	  ▪ ECDHE RSA with AES128-CBC and SHA256
	  ▪ ECDHE RSA with AES128-CBC and SHA
	  ▪ ECDHE RSA with AES256-GCM and SHA384

	▪ ECDHE RSA with AES256-CBC and SHA384 ▪ ECDHE RSA with AES256-CBC and SHA o For data at rest stored in the NinjaOne platform backend, FIPS 140-2 compliant cryptographic modules are utilized for encryption at rest. The data is encrypted with a minimum level of AES256, where higher strength cryptography may also be utilized as required.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • NIST SP # 800-39, Managing Information Security Risk • NIST SP # 800-41, Guidelines on Firewalls and Firewall Policy • NIST SP # 800-154, Guide to Data-Centric System Threat Modeling • NIST SP # 800-128, Guide for Security-Focused Configuration Management of Information Systems • NIST SP # 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs)

	• NIST SP # 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) • NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP # 800-34, Contingency Planning Guide for Federal Information Systems • NIST SP # 800-61, Computer Security Incident Handling Guide • NIST SP # 800-184, Guide for Cybersecurity Event Recovery • NIST SP # 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops • NIST SP # 800-86, Guide to Integrating Forensic Techniques into Incident Response • Using Amazon Web Services for Disaster Recovery, AWS October 2011 • Disaster Recovery with Amazon Web Services: A Technical Guide, Accenture June 2016 • Architecting for the Cloud: AWS Best Practices, AWS October 2018 • AWS Well-Architected Framework, AWS July 2019 • Affordable Enterprise-Grade Disaster Recovery Using AWS, CloudEndure/AWS 2019 • Backup strategy (online/offline; on-site/off-site), Uninterruptible power supply (UPS), Virus protection, Firewall, Reporting channels, Emergency plans
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	• Using Amazon Web Services for Disaster Recovery, AWS October 2011 • Disaster Recovery with Amazon Web Services: A Technical Guide, Accenture June 2016 • Architecting for the Cloud: AWS Best Practices, AWS October 2018

	• AWS Well-Architected Framework, AWS July 2019 • Affordable Enterprise-Grade Disaster Recovery Using AWS, CloudEndure/AWS 2019 • Backup (online/offline; on-site/off-site), Rapid recoverability
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures	• NIST SP # 800-55, Performance Measurement Guide for Information Security • NIST SP # 800-115, Technical Guide to Information Security Testing and Assessment • NIST SP # 800-154, Guide to Data-Centric System Threat Modeling • NIST SP # 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities • NIST SP # 800-192, Verification and Test Methods for Access Control Policies/Models • NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • Data protection management, Incident response management, order control (clear contract design, formalized order management, strict selection of service providers, follow-up checks)
Measures for user identification and authorisation	• NIST SP # 800-178, A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications • NIST SP # 800-192, Verification and Test Methods for Access Control Policies/Models • NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP # 800-92, Guide to Computer Security Log Management

	• NIST SP # 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) • Authorization concepts and needs-based access rights, Logging of accesses, Use of encryption methods, Disk management, Limitation of the number of administrators
Measures for the protection of data during transmission	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • For data in transit between the NinjaOne Agent and the NinjaOne platform, FIPS 140-2 compliant cryptographic modules enforced via TLS encryption. o Specifically, all ciphers are Perfect-Forward Secrecy (PFS), with the following cryptography: ▪ ECDHE RSA with AES128-GCM and SHA256 ▪ ECDHE RSA with AES128-CBC and SHA256 ▪ ECDHE RSA with AES128-CBC and SHA ▪ ECDHE RSA with AES256-GCM and SHA384

	▪ ECDHE RSA with AES256-CBC and SHA384 ▪ ECDHE RSA with AES256-CBC and SHA
Measures for the protection of data during storage	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • For data at rest in the NinjaOne platform backend, FIPS 140-2 compliant cryptographic modules are utilized for encryption at rest. The data is encrypted with a minimum level of AES256, where higher strength cryptography may also be utilized as required. • Multi-client capability, Sandboxing, Physically separated storage on separate folder structures, Client separation, Authorization concepts, Database rights
Measures for ensuring physical security of locations at which personal data are processed	• NIST SP # 800-30, Guide for Conducting Risk Assessments • NIST SP # 800-39, Managing Information Security Risk • NIST SP # 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations • NIST SP # 800-137, Information Security Continuous Monitoring

	(ISCM) for Federal Information Systems and Organizations Further, NinjaOne controls physical access by: 1) Deploying applications and backend systems to secured, audited, and well-regarded cloud service providers, not a NinjaOne-owned server. 2) Restricting access to NinjaOne offices only to employees, contractors, and invited guests (uninvited guests are asked to leave or to schedule a future visit if one is required). 3) Maintaining professional management of NinjaOne offices by vetted landlords and property management firms. 4) Requiring the use of keys, key cards, electronic key fobs, or mobile device tokens for entry into a NinjaOne offices. 5) Defining an office manager for each NinjaOne office, where each respective NinjaOne Office Manager will inventory, issue, and manage all keys, key cards, and fobs while recording all assignments of keys and fobs into an official log. 6) Requiring that any lost or stolen keys, key cards, or fobs must be reported to the NinjaOne Office Manager immediately, upon which time the keys, key cards, or fobs will be disabled. 7) Requiring that invited visitors to NinjaOne must check-in with the NinjaOne Office Manager who will maintain an Official Visitor Log recording the visitor's name, identification number,

	association, the purpose of visit, and the date and time of visit. 8) Requiring that all invited visitors must be escorted throughout the office. 9) Requiring that all invited visitor passes expire at the end of the day, on the same day of issuance. 10) Requiring that all NinjaOne employees will make every effort to maintain an orderly work environment that is void of clutter and exposure of proprietary or sensitive information. 11) Requiring that unused files in common areas should be shredded or locked in a file cabinet at the end of the day. 12) Recording the entrance and exit of all visitors and staff through any of the available doors, and keeping these for a minimum of 30 days. 13) Promptly revoking all key cards, tokens, and physical access to any staff that have left voluntarily or have been terminated.
Measures for ensuring events logging	• NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP # 800-92, Guide to Computer Security Log Management • NIST SP # 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) Further, NinjaOne: 1) Leverages a 24x7 Security Operations Center through an

	industry-trusted external security services provider. 2) Deploying realtime monitoring, auditing, and alerting of: a. network ingress b. network egress c. file alterations d. configuration changes e. successful and failed logins f. command execution g. application execution h. privileged execution i. OS vulnerabilities j. software vulnerabilities k. policy changes l. all-new activity m. atypical activity 3) Maintaining the logs and events captured for a minimum of one-year, and as necessary, up to an indefinite period of time.
Measures for ensuring system configuration, including default configuration	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • NIST SP # 800-36, Guide to Selecting Information Technology Security Products

	• NIST SP # 800-128, Guide for Security-Focused Configuration Management of Information Systems • NIST SP # 800-40, Guide to Enterprise Patch Management Technologies
Measures for internal IT and IT security governance and management	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • NIST SP # 800-39, Managing Information Security Risk • NIST SP # 800-41, Guidelines on Firewalls and Firewall Policy • NIST SP # 800-154, Guide to Data-Centric System Threat Modeling • NIST SP # 800-128, Guide for Security-Focused Configuration Management of Information Systems • NIST SP # 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs) • NIST SP # 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) • NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP # 800-34, Contingency Planning Guide for Federal Information Systems

	• NIST SP # 800-61, Computer Security Incident Handling Guide • NIST SP # 800-184, Guide for Cybersecurity Event Recovery • NIST SP # 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops • NIST SP # 800-86, Guide to Integrating Forensic Techniques into Incident Response
Measures for certification/assurance of processes and products	Annual examinations and testing of compliance and security controls through the AICPA Service Organization Control (SOC 2) process of testing Trust Service Principles. The AICPA SOC 2 examination includes 144 [out of 150] individual controls that overlap with the ISO27001 standard.
Measures for ensuring data minimisation	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • NIST SP # 800-39, Managing Information Security Risk • NIST SP # 800-41, Guidelines on Firewalls and Firewall Policy • NIST SP # 800-154, Guide to Data-Centric System Threat Modeling • NIST SP # 800-128, Guide for Security-Focused Configuration Management of Information Systems

	• NIST SP # 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs) • NIST SP # 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) • NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP # 800-34, Contingency Planning Guide for Federal Information Systems • NIST SP # 800-61, Computer Security Incident Handling Guide • NIST SP # 800-184, Guide for Cybersecurity Event Recovery • NIST SP # 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops • NIST SP # 800-86, Guide to Integrating Forensic Techniques into Incident Response
Measures for ensuring data quality	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • NIST SP # 800-39, Managing Information Security Risk • NIST SP # 800-41, Guidelines on Firewalls and Firewall Policy • NIST SP # 800-154, Guide to Data-Centric System Threat Modeling

	• NIST SP # 800-128, Guide for Security-Focused Configuration Management of Information Systems • NIST SP # 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs) • NIST SP # 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) • NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP # 800-34, Contingency Planning Guide for Federal Information Systems • NIST SP # 800-61, Computer Security Incident Handling Guide • NIST SP # 800-184, Guide for Cybersecurity Event Recovery • NIST SP # 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops • NIST SP # 800-86, Guide to Integrating Forensic Techniques into Incident Response
Measures for ensuring limited data retention	• NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP # 800-34, Contingency Planning Guide for Federal Information Systems • Using Amazon Web Services for Disaster Recovery, AWS October 2011 • Disaster Recovery with Amazon Web Services: A Technical Guide, Accenture June 2016 • Architecting for the Cloud: AWS Best Practices, AWS October 2018 • AWS Well-Architected Framework, AWS July 2019

	• Affordable Enterprise-Grade Disaster Recovery Using AWS, CloudEndure/AWS 2019
Measures for ensuring accountability	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • NIST SP # 800-39, Managing Information Security Risk • NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP # 800-92, Guide to Computer Security Log Management • NIST SP # 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)
Measures for allowing data portability and ensuring erasure	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering

	• NIST SP # 800-35, Guide to Information Technology Security Services
	• NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems
	• NIST SP # 800-95, Guide to Secure Web Services
	• NIST SP # 800-123, Guide to General Server Security
	• NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing
	• NIST SP # 800-160, Systems Security Engineering
	• For data in transit between the NinjaOne Agent and the NinjaOne platform, FIPS 140-2 compliant cryptographic modules enforced via TLS encryption.
	  ○ Specifically, all ciphers are Perfect-Forward Secrecy (PFS), with the following cryptography:
	  ▪ ECDHE RSA with AES128-GCM and SHA256
	  ▪ ECDHE RSA with AES128-CBC and SHA256
	  ▪ ECDHE RSA with AES128-CBC and SHA
	  ▪ ECDHE RSA with AES256-GCM and SHA384
	  ▪ ECDHE RSA with AES256-CBC and SHA384
	  ▪ ECDHE RSA with AES256-CBC and SHA
	• For data at rest in the NinjaOne platform backend, FIPS 140-2 compliant cryptographic modules are utilized for encryption at rest. The data is encrypted with a minimum level of AES256, where

	higher strength cryptography may also be utilized as required. • NIST SP # 800-111, Guide to Storage Encryption Technologies for End User Devices • NIST SP # 800-124, Guidelines for Managing the Security of Mobile Devices in the Enterprise
For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • NIST SP # 800-39, Managing Information Security Risk • NIST SP # 800-41, Guidelines on Firewalls and Firewall Policy • NIST SP # 800-154, Guide to Data-Centric System Threat Modeling • NIST SP # 800-128, Guide for Security-Focused Configuration Management of Information Systems • NIST SP # 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs) • NIST SP # 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) • NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP # 800-34, Contingency Planning Guide for Federal Information Systems

	• NIST SP # 800-61, Computer Security Incident Handling Guide • NIST SP # 800-184, Guide for Cybersecurity Event Recovery • NIST SP # 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops • NIST SP # 800-86, Guide to Integrating Forensic Techniques into Incident Response