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 NinjaRMM, LLC, a Delaware Limited Liability Company located at 500 N. Brand, Glendale CA 91203 ("**NinjaRMM**") and the company, specified in the signature block ("**Customer**") (each a "**Party**", and collectively, the "**Parties**").

WHEREAS, NinjaRMM is a SaaS based multi-tenant RMM platform and provides services to the Customer ("**Services**").

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

WHEREAS, in the provision of the Services under the Agreement, NinjaRMM may process certain personal data ("**Personal Data**") on behalf of the Customer, such data being made available by the Customer 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:

"**Affiliates**" means a company, person or entity that is owned or controlled by, that owns or controls or is under common ownership or control with a Party. Ownership shall mean direct or indirect ownership of more than 50% of the shares in a company or entity, and control shall mean any power to appoint persons to the board of directors of a company or entity;

"**Applicable Data Protection Law**" shall mean 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 and all other applicable laws and regulations in any relevant jurisdiction relating to the processing of personal data and privacy (such as, without limitation, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector as may be amended from time to time);

"**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

The Customer's data are processed within distinct and separate domains and for separate purposes:

3.1 **Customer Data**: The provisions of this DPA shall apply to the extent NinjaRMM processes, on behalf of the Customer, any Personal Data provided by the Customer, directly or indirectly, in connection with the Agreement as described in the Schedule attached to this DPA (the "**Customer Data**"), provided, however, that the data listed in Sec. 3.1 and 3.2 below are not processed on behalf of the Customer, but on a controller-to-controller-basis.

3.2 "**Organization Customer Relationship Data**" is any information necessary for: contact and communications, sales and marketing, and billing, payment and invoicing. This would include Personal Data. Such Organization Customer Relationship Data are not used within the NinjaRMM Application/Platform and are not transferred nor stored within the NinjaRMM Application/Platform. Such Organization Customer Relationship Data are further not governed by the provisions of this DPA, meaning that NinjaRMM does not process such data on behalf of the Customer. Rather, the Customer and NinjaRMM act as independent controllers when processing such Organization Customer Relationship Data. The transfer of such data by the Customer to NinjaRMM and NinjaRMM's use of such data is based on Art. 6(I)(1)(f) GDPR (legitimate interests) and is required for the performance of the Agreement and/or the pursuit of other legitimate interests.

3.3 "**NinjaRMM Application/Platform Troubleshooting Data**" is comprised by these two types and is used for the following purposes:

- Type 1) Troubleshooting information for endpoints and systems:
    - CPU performance, load, and utilization
    - Memory capacity, usage, and/or exhaustion
    - Hard drive and I/O performance, parameters, and errors
    - Network metrics, utilization, and errors
    - Operating system notifications and events
    - Hardware configurations and manufacturer identification

- Type 2) Troubleshooting information for software and applications:
    - Error codes and messages
    - Debug information
    - Code snippets that are part of errors and debug information

- Issue-relevant software configurations, versions, and vendor IDs

The NinjaRMM Application/Platform Troubleshooting Data, to the extent used for NinjaRMM's troubleshooting activities, are not governed by the provisions of this DPA, meaning that NinjaRMM does not process such data on behalf of the Customer. Rather, the Customer and NinjaRMM act as independent controllers when processing such NinjaRMM Application/Platform Troubleshooting Data. The transfer of such data by the Customer to NinjaRMM and NinjaRMM's use of such data is based on Art. 6(I)(1)(f) GDPR (legitimate interests) and is required for the performance of the Agreement and/or the pursuit of other legitimate interests, in particular the performance of NinjaRMM's troubleshooting activities.

NinjaRMM Application/Platform Troubleshooting Data is maintained, transferred within, and stored within EU borders. Any and all of the NinjaRMM Application/Platform Troubleshooting Data is transferred and stored encrypted within EU borders with FIPS 140-2 compliant cryptographic modules.

ONLY by expressed request from the Customer, or by expressed requirement from the Customer, shall transfer NinjaRMM Application/Platform Troubleshooting Data outside of EU borders.

4. Processing of Personal Data

4.1 NinjaRMM processes the Customer Data on behalf of the Customer and acts as processor and the Customer acts as controller. Customer Data may include Personal Data relating to users or end-users of the Customer. Processing may include processing by NinjaRMM or any of its Affiliates acting as NinjaRMM's subcontractors.

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, NinjaRMM shall:

(a) Treat the Customer Data as confidential information and process the Customer Data solely and exclusively for the purpose of providing Services to the Customer and on Customer's behalf. The processing by NinjaRMM shall consist of all permitted processing operations as stipulated in this DPA or in the Agreement. The categories of Personal Data to be processed by NinjaRMM will be limited to the Customer Data that are necessary to deliver the Services to the Customer. The duration of the processing by NinjaRMM is limited to the duration described in the Agreement or this DPA.

(b) NinjaRMM 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. NinjaRMM shall not 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 NinjaRMM would be required by any applicable legislation to process any Customer Data otherwise than as permitted herein, NinjaRMM shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. NinjaRMM 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. NinjaRMM shall be entitled to suspend the provisions of Services that it suspects to infringe the Applicable Data Protection Law until the Customer confirms or amends its instruction in writing. NinjaRMM shall be entitled to reject instructions of the Customer that are obviously illegal and/or violate the Applicable Date Protection Law.

(c) Implement appropriate and sufficient, 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 any form of accidental, unlawful or unauthorized processing. In particular, without limitation, NinjaRMM 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 any form of unlawful processing. NinjaRMM 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. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
ii. The ability 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 ensuring 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 shall remain in place throughout the duration that NinjaRMM provides Services to the Customer or until NinjaRMM ceases to process Customer Data (whichever is later);

(d) Treat Customer Data with strict confidence and take all appropriate steps to ensure that disclosure of or access to Customer Data is restricted to its employees, consultants or agents that strictly require such Customer Data to perform the tasks allotted to them by NinjaRMM in the performance of NinjaRMM's obligations under the Agreement (the "Authorized Persons") and excluding all access to Customer Data which are not strictly necessary for the Authorized Persons to perform its part of the Services. NinjaRMM shall ensure 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. NinjaRMM shall ensure that such confidentiality obligations survive the termination of the employment or contracting agreement;

iii. Have received appropriate training in relation to the Applicable Data Protection Law;

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 and in accordance with the Customer's instructions.

(e) 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 NinjaRMM is prohibited to do so by court or by order of the competent authority. NinjaRMM shall immediately inform the competent authorities that the usage of the Customer Data is at the sole discretion of the Customer.

(f) In the frame of the Parties' relationship as of the date of this DPA, the Customer authorizes NinjaRMM to be assisted by subcontractors strictly with a view to deliver and improve the agreed Services, provided NinjaRMM has contracted with said subcontractors with terms substantially similar to the ones included herein. When the use of subcontractors does not fall within the scope of the present general authorization, NinjaRMM shall inform the Customer at least one month in advance and by means of a written communication about its intention to engage a subcontractor, including details on the identity of the subcontractor, the location where the Customer Data will be processed by such subcontractor and the concerned data processing activities. NinjaRMM will enter into written contracts with such subcontractors ("**Approved Sub-processor**"), guaranteeing at least a level of data protection and information security as provided for herein and in any event NinjaRMM will remain fully liable to the Customer for any breach of the Approved Sub-processor that is caused by an act, error or omission of the Approved Sub-processor. NinjaRMM shall maintain and provide upon reasonable request a copy of the list of concerned subcontractors. The Customer shall have the right to object against the use of a subcontractor pursuant to article 28 para 2 of the GDPR.

(g) The Customer hereby approves the following sub-contractors as Approved Sub-processor.

Amazon Web Services (AWS), with AWS GDPR DPA:
https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

5. International transfers of Personal Data

NinjaRMM 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**").

NinjaRMM implements and enforces data protection through compliance and security controls that are based upon the strict requirements within the following frameworks and guidelines:

- 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

NinjaRMM undergoes 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.

In addition, NinjaRMM models the United States Cybersecurity Maturity Model Certification (CMMC) standard, Level 3. Specifically, CMMC Level 3 includes 110 security requirements specified in NIST SP 800-171.

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 Personal Data, which are subject to this DPA from the Customer to NinjaRMM, the Parties hereby enter into the EU Standard Contractual Clauses which are attached hereto as Schedule 3. 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.

6. Duty to Notify and Cooperate

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

(a) if for any reason (i) NinjaRMM 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 NinjaRMM. In such cases, NinjaRMM 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 necessary 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 NinjaRMM;

(c) upon becoming aware of any data breach. In such case, NinjaRMM 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. NinjaRMM shall further take all such 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 all 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. NinjaRMM 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. NinjaRMM 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 NinjaRMM provides to demonstrate compliance with this DPA or Applicable Data Protection Law.

In addition to the foregoing, if NinjaRMM 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) cooperate, at its own expense, as 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 NinjaRMM under this DPA. NinjaRMM 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 NinjaRMM and shall provide all details thereof. Furthermore, NinjaRMM 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. NinjaRMM understands that any response to such direct requests requires prior written authorization from the Customer. If necessary, NinjaRMM shall co-operate with the competent supervisory authority;

(f) upon the Customer's 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. In particular, the Customer or a third party appointed by the Customer (the "**Auditor**") may enter NinjaRMM's premises and more specifically the rooms or locations where the Customer Data is processed by NinjaRMM to verify NinjaRMM's compliance hereunder, provided that such inspection shall be carried out with reasonable notice (except where such notice would defeat the purpose of the audit) during regular business hours and under a duty of confidentiality. The Customer or the Auditor may inspect, audit and copy any relevant records, processes and systems to verify compliance with the Applicable Data Protection Law and this DPA. The Customer shall take all reasonable measures to prevent unnecessary disruption to NinjaRMM'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 NinjaRMM.

7. Effect of Termination

As soon as it is no longer required for the performance of the Services and at the latest upon the expiration or termination of the Agreement, NinjaRMM shall promptly notify the Customer of all Customer Data in its possession and delete all such Customer Data and any existing copies thereof, at NinjaRMM's sole expense, unless any applicable law requires the further storage of the Customer Data. At the Customer's request, NinjaRMM shall certify to the Customer that all Customer Data has been destroyed in accordance with the foregoing. If NinjaRMM cannot destroy or delete the Customer Data due to technical reasons, NinjaRMM 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. Liability

The liability provisions of the Agreement shall apply accordingly to this DPA.

9. Order of Precedence

In the event of a conflict between the provisions of this DPA and those of the Agreement in respect of the processing and protection of Customer Data, the provisions of this DPA will prevail. Except as expressly modified herein, all terms and conditions of the Agreement shall remain in full force and effect. The EU Standard Contractual Clauses which are attached hereto as Schedule 3 shall prevail over any other provisions of the Agreement and the DPA.

10. Governing Law

Notwithstanding anything in the Agreement to the contrary, this DPA will be governed exclusively by and interpreted in accordance with the laws of the State of Delaware, excluding any conflicts of law principles. All disputes arising out or in connection with this DPA will be submitted exclusively to the competent courts of Los Angeles, California, whether federal or state. The provisions of the EU Standard Contractual Clauses which are attached hereto as Schedule 3 shall remain unaffected.

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

NINJARMM, LLC	**[CUSTOMER]**
BY:_____	BY:_____
ITS:_____	ITS:_____
DATE:_____	DATE:_____
–	–

Schedule 1: Data Processing Schedule

1. Categories of Data

The Customer Data processed by NinjaRMM on behalf of the Customer in connection with the Services provided by NinjaRMM 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):

- Email address of the primary NinjaRMM account owner
- Email addresses of system administrators authorized by the NinjaRMM Customer to use the NinjaRMM Application
- IP address(es) for a NinjaRMM Customer's datacenter IP address(es) for a NinjaRMM Customer's headquarters/satellite offices
- IP address(es) for equipment/devices belonging to the NinjaRMM Customer and/or their clients: laptops, desktops, servers, network devices
- System names for equipment/devices belonging to the NinjaRMM Customer and/or their clients: laptops, desktops, servers, network devices
- Hardware details of equipment/devices belonging to the NinjaRMM Customer and/or their clients: laptops, desktops, servers, network devices
- Software details of equipment/devices belonging to the NinjaRMM Customer and/or their clients: laptops, desktops, servers, network devices
- Usernames belonging to the NinjaRMM Customer and/or their clients
- Browser/user-agent details belonging to the NinjaRMM Customer
- Performance and utilization metrics of equipment/devices belonging to the NinjaRMM Customer and/or their clients: laptops, desktops, servers, network devices
- Error codes of equipment/devices belonging to the NinjaRMM Customer and/or their clients: laptops, desktops, servers, network devices

2. Categories of data subjects

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

3. Permitted processing operations for NinjaRMM

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

4. Permitted Purposes

NinjaRMM 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 NinjaRMM 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.

Schedule 2: Organizational and technical measures (TOM)

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

- Ensure ongoing confidentiality, integrity, availability and resilience of processing systems.
- Review and audit vendors regarding data privacy standards.
- Provide audited physical, virtual and organizational access control.
- Audit of employee data access behavior.
- Secure data via physical and virtual security systems.
- Processes to regularly test, assess and evaluate effectiveness of TOMs.
- Anonymize data where no Personal Data is needed.
- Encryption of all data streams with FIPS 140-2 compliant cryptographic models.
- Compliance and security controls that are based upon the strict requirements within the following frameworks and guidelines e.g.
    - 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
- 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.

Schedule 3: Standard Contractual Clauses (Controller to Processor)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: Mentor IT A/S

Address: Lindevej 8, 6710 Esbjerg, Denmark

Tel.: +45 70 12 21 23 fax.: N/A e-mail: GDPR@Mentor-it.dk

Other information needed to identify the organisation: N/A

('the data **exporter**')

and

Name of the data importing organisation: NinjaRMM, LLC, a Delaware Limited Liability Company

Address: 500 N. Brand, Glendale CA 91203

Tel.: fax: e-mail:

Other information needed to identify the organisation:

('the data **importer**')

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i.) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii.) any accidental or unauthorised access; and

(iii.) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of

the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations, referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the

same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely Denmark

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually

disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely

4. The data exporter shall keep a list of sub-processing agreements executed under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full): Jesper Ungermann Christensen

Position: Quality Assurance & Compliance Manager

Address: Lindevej 8, 6710 Esbjerg, Denmark

Other information necessary in order for the contract to be binding (if any):

Signature: Jesper U. Christensen

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Lewis Huynh

Position: Chief Security Officer

Address: 26750 US Highway 19 North, Clearwater, FL 33761

Other information necessary in order for the contract to be binding (if any):

Signature:

(stamp of organisation)

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

IT MSP, providint IT-outsourcing services, such as Patch Management of units,

Managed Anti-Virus solutions etc.

Data importer

The data importer is (please specify briefly your activities relevant to the transfer):

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

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

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

Categories of data

The personal data transferred concern the following categories of data (please specify):

The Customer Data processed by NinjaRMM on behalf of the Customer in connection with the Services provided by NinjaRMM 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):

- Email address of the primary NinjaRMM account owner

- Email addresses of system administrators authorized by the NinjaRMM Customer to use the NinjaRMM Application
- IP address(es) for a NinjaRMM Customer's datacenter IP address(es) for a NinjaRMM Customer's headquarters/satellite offices
- IP address(es) for equipment/devices belonging to the NinjaRMM Customer and/or their clients: laptops, desktops, servers, network devices
- System names for equipment/devices belonging to the NinjaRMM Customer and/or their clients: laptops, desktops, servers, network devices
- Hardware details of equipment/devices belonging to the NinjaRMM Customer and/or their clients: laptops, desktops, servers, network devices
- Software details of equipment/devices belonging to the NinjaRMM Customer and/or their clients: laptops, desktops, servers, network devices
- Usernames belonging to the NinjaRMM Customer and/or their clients
- Browser/user-agent details belonging to the NinjaRMM Customer
- Performance and utilization metrics of equipment/devices belonging to the NinjaRMM Customer and/or their clients: laptops, desktops, servers, network devices
- Error codes of equipment/devices belonging to the NinjaRMM Customer and/or their clients: laptops, desktops, servers, network devices

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Not Applicable.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

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

DATA EXPORTER

Name: Jesper Ungermann Christensen

Authorised Signature Jesper U. Christensen

DATA IMPORTER

Name: NinjaRMM, LLC, a Delaware Limited Liability Company

Authorised Signature

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

- Ensure ongoing confidentiality, integrity, availability and resilience of processing systems.
- Review and audit vendors regarding data privacy standards.
- Provide audited physical, virtual and organizational access control.
- Audit of employee data access behavior.
- Secure data via physical and virtual security systems.
- Processes to regularly test, assess and evaluate effectiveness of TOMs.
- Anonymize data where no Personal Data is needed.
- Encryption of all data streams with FIPS 140-2 compliant cryptographic models.
- Compliance and security controls that are based upon the strict requirements within the following frameworks and guidelines e.g.
    - 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
- 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.