Partner Data Protection Addendum

This Partner Data Protection Addendum (this "**Addendum**"), effective as of the last date signed below ("**Effective Date**") entered into by and between **Akamai Technologies Inc**., with its principle place of business at 145 Broadway, Cambridge MA,02142, USA, **Akamai Technologies Ltd**., with its principle place of business at 5 New Street Square, London EC4A 3TW, UK, **Akamai Technologies Israel Ltd.**, with its principal place of business at Hamada 3West Building 2nd Floor, Herzliya 467333, Israel and **Akamai Technologies International AG**, with its principle place of business at Löwenstrasse 1, 8001 Zürich, Switzerland (each separately "**Akamai**") and **Danidin Ltd**., with its principle place of business at Zinonos Kitieos 9, Egkomi, P.C. 2406 Nicosi, Cyprus, **Globaldots Russia LLC**, with its principle place of business at 117246 Moscow, Nauchniy proezd, bld.19, **GlobalDots Inc.**, with its principle place of business at 919 North Market Street, Suite 950 Wilmington, DE 19801, USA and **Tango Sierra Ltd**., with its principle place of business at c/o Cohen & Cohen 3 Tel-Aviv Street, 3541629 Haifa, Israel, GlobalDots, Inc., with its principle place of business at 919 North Market Street, Suite 950 Wilmington, DE 19801, USA (each separately "**Partner**"), supplements and amends, as necessary, the sales terms and conditions (as amended, the "**Channel Agreement**") entered into by and between **Akamai** and **Partner** on or prior to the date hereof. If the provisions of this Addendum and the Channel Agreement conflict, then the provisions of this Addendum shall control. Unless otherwise defined herein, all capitalized terms used herein shall have the meanings assigned to such terms in the Channel Agreement.

This Addendum replaces the Data Protection Addendum signed on February 25, 2020.

NOW, THEREFORE, in consideration of the following as set forth in this Addendum, the parties hereby agree as follows:

1. Definitions

"Agreement Personal Data"	means all Personal Data that Akamai processes on behalf of Partner as a data processor, as specified in Schedule 1..
"Authorised Sub-Processor"	means Akamai, and any third party appointed by Akamai in accordance with this Addendum to process Agreement Personal Data, for which Akamai serves as a processor or sub-processor, on behalf of and as instructed by Akamai. For the avoidance of doubt, suppliers to Akamai responsible for the transit of communications through Akamai servers located in server colocation and bandwidth connectivity providers around the world, where such providers have no access to such communications nor any data

MM

	located on Akamai operated servers (i.e. "mere conduits"), shall not be considered Authorised Sub-Processors.
"Cross-Border Transfer Mechanism"	means applicable legal mechanisms required for the transfer of Personal Data from a Data Controller or Data Processor in a given jurisdiction to another Data Controller or Data Processor operating in a separate jurisdiction where applicable Data Protection Laws require a legal mechanism for cross-border transfer. Such mechanisms include, by way of example and without limitation, adequacy decisions, binding corporate rules, the EU standard contractual clauses for Data Processors established in third countries pursuant to European Regulation (2016/679) under the EU Directive (95/46/EC), as may be updated or replaced from time to time.
"Data Protection Laws"	means all applicable laws (including decisions and guidance by relevant Supervisory Authorities) relating to data protection, the processing of personal data, and privacy applicable to Akamai and the Partner in respect of the processing of Agreement Personal Data to provide the Services, including such laws, by way of example and without limitation, the General Data Protection Regulation, the California Consumer Privacy Act, and the Personal Information Protection and Electronic Documents Act
"Data Breach Incident"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Agreement Personal Data transmitted, stored or otherwise Processed.
"Supervisory Authorities"	means any applicable authority that oversees compliance with the Data Protection Laws, including as defined in GDPR.

2. Data Protection

2.1 **Roles and Compliance with Law.** For the purpose of this Agreement it is understood that the Partner considers itself to act on behalf of its Client as a data processor (and the Partner's Client to act as the ultimate data controller) and Akamai is an Authorized Sub-Processor under this Agreement**.** Both the Partner and Akamai shall comply with their respective obligations under the Data Protection Laws.

2.2 **Data Processor Terms.** The parties agree and acknowledge that Akamai, and any relevant Akamai Affiliates, when providing the Services for Partner and/or Partner's Client, will be acting as an Authorized Sub Processor (on behalf of Partner as a Data Processor) in respect of the processing by or for it of Agreement Personal Data.

Partner (A) authorizes Akamai to process the Agreement Personal Data, and (B) confirms that on the effective date of each respective Order Form made after the Effective Date hereof Partner will have obtained its Client's consent for Akamai to process such Agreement Personal Data and its Client has confirmed it will have obtained enduser consent or has another legal basis for processing, as applicable, in each case for the term of any applicable Order Form under the Channel Agreement as a Data Processor or Authorised Sub-Processor as applicable (on its and its Affiliates behalf) for the purposes of providing the Services only.

2.2.1 Akamai is authorised to engage, use or permit an Authorised Sub-Processor for the Processing of Agreement Personal Data provided that:

(a) Akamai undertakes reasonable due diligence on them in advance to ensure appropriate safeguards for Agreement Personal Data and individual rights in accordance with applicable Data Protection Laws;

(b) Akamai shall provide Partner with advance written notice of any intended changes to any Authorised Sub-Processor, allowing Partner sufficient opportunity to object;

(c) Akamai has entered into a data processing agreement with such Authorized Sub-Processor that satisfies the requirements of the applicable Data Protection Laws and the terms of this Agreement; and

(d) The Authorised Sub-Processor's activities must be specified in accordance with the obligations set out in this Section 2.2.

Without prejudice to this Section 2.2.1, Akamai shall remain responsible for all acts or omissions of the Authorised Sub-Processor as if they were its own.

2.2.2 Akamai shall (and procure that any Authorised Sub-Processor shall):

(a) process the Agreement Personal Data only on documented instructions from Partner, including the Channel Agreement, any technical specifications provided for administration of the Services, and configuration settings set by Partner or Partner's Client in any of Akamai's customer portals provided for administration of the Services;

(b) without prejudice to Section 2.2.2(a), ensure that Agreement Personal Data will only be used by Akamai as set forth in the Channel Agreement;

(c) ensure that any persons authorised to process the Agreement Personal Data:

(a) have committed themselves to appropriate confidentiality obligations in relation to Agreement Personal Data or are under an appropriate statutory obligation of confidentiality;

(b) access and process the Agreement Personal Data solely on written documented instructions from Partner; and

(c) are appropriately reliable, qualified and trained in relation to their processing of Agreement Personal Data;

(d) implement technical and organisational measures at a minimum to the standard set out in the Schedule 2 to ensure a level of security appropriate to the risk presented by processing the Agreement Personal Data, in particular from a Data Breach Incident;

(e) notify Partner without undue delay (and in any event no later than 48 hours) after becoming aware of a Data Breach Incident as set forth in Section 5;

(f) assist Partner in:

(a) responding to requests for exercising the Data Subject's rights under the Data Protection Laws, by appropriate technical and organisational measures, insofar as this is possible, provided that Akamai shall not be required to store or process any data for the purpose of re-identifying an individual when such information is not normally processed or stored by Akamai;

(b) reporting any Data Breach Incident to any Supervisory Authority or Data Subjects and documenting any Data Breach Incidents;

(c) taking measures to address the Data Breach Incident, including, where appropriate, measures to mitigate its possible adverse effects; and

(d) conducting mandatory privacy impact assessments of any processing operations and consulting with any applicable Supervisory Authority or appropriate persons accordingly;

(g) at the choice of Partner, to the extent that Agreement Personal Data is stored by Akamai, securely delete or return all Agreement Personal Data to Partner after the end of the provision of relevant Services relating to processing, and securely delete any remaining copies and certify when this exercise has been completed;

(h) make available to Partner all information necessary to comply with its obligations to do so under the Data Protection Laws and allow for and contribute to audits, including inspections, conducted by Partner or another auditor mandated by Partner (including in response to audit requests by Partner's Client);

(i) acquire no rights or interest in the Agreement Personal Data, except to the extent necessary to provide the Services under the respective contract; and

(j) not transfer any Agreement Personal Data outside of the EEA, except as provided for in Section 2.3 below.

2.3 **Transfers Outside of the EEA.**

2.3.1 The Partner hereby acknowledges and accepts that the Akamai platform is made up of servers owned and operated by Akamai and/or its Affiliates globally and that Akamai processes Agreement Personal Data not only in the applicable jurisdiction(s) where the Partner or Partner's Clients operate, but also transfers Agreement Personal Data outside of such jurisdictions, dependent upon the location of the Partner's or the Client's end user and the Akamai servers serving those connections (subject to clause 2.2(a) above). Such cross-border transfers shall take place in accordance with applicable Data Protection Laws, including, without limitation, completing any required prior assessments. A list of all countries in which Akamai operates servers, including a list of all Akamai Affiliates that own such servers, as may be updated from time to time, is available in Akamai's Privacy Trust Centre at https://www.akamai.com/us/en/multimedia/documents/akamai/points-of-presence-countries.pdf.

2.3.2 To the extent that Agreement Personal Data is subject to a cross-border transfer to a non-EU member country that does not have an EU adequacy determination, at least one of the Cross-Border Transfer Mechanism(s) listed below shall apply in the order of preference listed in the event that more than one mechanism applies:

(a) Binding Corporate Rules -- To the extent Akamai has adopted Binding Corporate Rules, it shall maintain such Binding Corporate Rules and promptly notify the Partner in the event that the Binding Corporate Rules are no longer a valid transfer mechanism between the parties.

(b) EU Standard Contractual Clauses (processors) -- To the extent applicable, the EU standard contractual clauses for the transfer of personal data tothird countries pursuant to EU Regualation (2016/679) under the EU Directive (95/46/EC), and as may be updated or replaced from time to time ("Standard Clauses"), are hereby agreed between:

(a) Module 3 Processor to Processor (where Akamai as the data exporter transfers Agreement Personal Data to Akamai Technologies, Inc.) as data importer; and

(b) Module 3 Processor to Processor (where he Partner as Data Exporter transfers Agreement Pesonal Data to Akamai Technologies, Inc. as Data Importer.

A copy of the Akamai signed Standard Clauses is available in Akamai's Privacy Trust Center at www.akamai.com/compliance/privacy.

For the agreed Standard Clauses Appendix 1 of the Standard Clauses shall be deemed to be prepopulated with the relevant sections of Schedule 1 of this Agreement and Appendix 2 of the Standard Clauses shall be deemed to be prepopulated with Schedule 2 of this Agreement.
Upon acceptance of the Standard Clauses by the Partner, the Standard Clauses are incorporated into this Agreement.

MM

(c) And, as applicable, Module 3 (Processor to Processor) Akamai as Data Exporter and any non-Akamai party that is an Authorized Sub-Processors as Data Importer

Upon the Partners request, Akamai will provide a copy of the signed Standard Clauses between Akamai and the Authorized Sub-Processors.

2.3.3 In addition to the foregoing Section 2.3.2, any similarly applicable standard contractual clauses adopted by a Supervisory Authority or other body of competent jurisdiction to govern the cross-border transfer of Personal Data subject to applicable Data Protection Laws shall be incorporated herein by the parties hereto in accordance with their respective roles pursuant to such clauses as analogous to those set out in Section 2.3.2 (c). Such clauses shall be supplemented and/or prepopulated (as applicable) with the relevant sections of this Agreement and its appended Schedules. An Akamai pre-signed version of such clauses will be made available in the Privacy Trust Center at www.akamai.com/compliance/privacy.

3. Audits

Akamai shall conduct periodic audits of its processing of Agreement Personal Data to ensure compliance with applicable Data Protection Laws, including applicable organisational and technical measures necessary to protect Agreement Personal Data. Upon reasonable request, Akamai shall deliver to Partner relevant compliance documentation from such audit(s) (e.g., Akamai's then-current SOC 2 Type 2 (or its successor) report) and certain, selected policies, procedures and evidence that have been approved for distribution to customers.

4. Cooperation

Akamai shall reasonably cooperate with Partner to enable Partner to respond to any requests, complaints or other communications from Clients, data subjects and governmental, regulatory or judicial bodies relating to the processing of Agreement Personal Data under the Channel Agreement.

5. Data Breach Incidents

5.1 Akamai shall notify Partner without undue delay, after becoming aware of a Data Breach Incident by providing notice via e-mail to the 24-hour security contacts provided by Partner in Akamai's Luna Control Center customer portal. Where Akamai needs to notify a supervisory authority about an incident it will align its communication with the supervisory authority with the Partner as reasonable, permitted, and appropriate.

5.2 Furthermore, in the event of a Data Breach Incident, Akamai shall:

5.2.1 provide timely information and commercially reasonable cooperation so that the Partner may fulfil its obligations under applicable Data Protection Laws in regards, to any required notifications; and

5.2.2 take all commercially reasonable measures and actions as are appropriate to remedy or mitigate the effects of the Data Breach Incident and shall keep Partner (and

MM

where applicable the supervisory authority) up-to-date about all developments in connection with the Data Breach Incident.

6. Authorizations

The Partner hereby acknowledge and accepts that the Akamai platform is made up of servers owned and operated by Akamai or its Affiliates globally and that connections between a web property and one of its end users may be made through any of these servers dependant upon the location of the end user. A list of all countries in which Akamai operates servers, a list of all Akamai Affiliates that may own such servers, as may be updated from time to time, as well as a list of all sub-processors used by Akamai, can be found at www.akamai.com/compliance/privacy. Partner hereby consents to Akamai's use of listed sub-processor(s), subject to Akamai's compliance with the provisions of this Addendum with respect to Authorized Sub-Processors and transfer of Personal Data outside of the EEA. In addition, to the extent that any applicable Data Protection Laws would deem an Akamai Affiliate by virtue of its ownership of servers used to provide the services, to be a sub-processor for purposes of this Addendum, Partner hereby consents to Akamai's use of such sub-processor(s), subject to Akamai's compliance with the provisions of this Addendum with respect to Authorized Sub-Processors and transfer of Personal Data outside of the EEA.

7. Express Third Party Beneficiaries

The Parties hereby agree that Partner's Clients are intended and express third party beneficiaries of all of the provisions of this Addendum and shall have the right, exercisable in their discretion, to enforce the terms and conditions of this Addendum against the Parties, as applicable, or prevent the breach thereof, or to exercise any other right, or seek any other remedy, which may be available to it as a third-party beneficiary of this Addendum. For the avoidance of doubt, the terms of this Addendum, including the attached EU Standard Clauses, shall be enforceable by Partner's Clients as though executed directly by such parties.

For avoidance of doubt Partner's Clients shall be third party beneficiaries in the meaning of this section only in relation to their own Agreement Personal Data.

8. Miscellaneous

8.1 Except for the changes made by this Addendum, the Channel Agreement remains unchanged and in full force and effect. This Addendum may be executed in two or more counterparts, each of which shall be deemed an original and all of which taken together shall be deemed to constitute one and the same document. The parties may sign and deliver this Addendum by facsimile or email transmission.

8.2 The obligations placed upon the parties under this Addendum shall survive so long as Akamai possesses Agreement Personal Data processed as a result of Partner's or its Clients use of the Services.

8.3 This Addendum may not be modified except by a subsequent written instrument signed by both parties.

8.4 If any part of this Addendum is held unenforceable, the validity of all remaining parts will not be affected.

MM

IN WITNESS WHEREOF, the parties hereto have caused this Addendum to be duly executed and delivered by their respective authorized representatives as of the Effective Date.

AKAMAI TECHNOLOGIES LTD
AKAMAI TECHNOLOGIES ISRAEL LTD
AKAMAI TECHNOLOGIES INTERNATIONAL AG

By: _____

Name: Hans Nipshagen

Title: RVP, Channels & Alliances EMEA

Date: 22/02/2022

PARTNER:

By: _____

Name: Margarita Malai

Title: Group Legal Consultant

Date: 22 February 2022

AKAMAI TECHNOLOGIES, INC.

By: _____

Name: Hans Nipshagen

Title: RVP, Channels & Alliances EMEA

Date: 22/02/2022

Schedule 1 of the Data Processing Agreement:
Details of Akamai's Processing Activities

1. Data Processor

Akamai is a provider of content delivery, media acceleration, web performance and Internet security services.

2. Data Subjects

Akamai, when performing Services under the Channel Agreement, processes data on behalf of its:

- Partner, or

that may contain the Personal Data of the end users accessing Customer Content and/or using Partner's or Partner's Clients' services.
"Customer Content" means all content and applications, including any third-party content or applications, provided to Akamai in connection with Partner's or Partner's Clients' access to or use of the Services.

3. Categories of data processed

a) End User Personal Data

Akamai processes Personal Data included within Customer Content ("End User Personal Data") when providing the Services under the Channel Agreement. Upon the Partner or Partner's Client choice, End User Personal Data may include data such as:

a. Login credentials;

b. Subscriber name and contact information;

c. Financial or other transaction information;

d. Other Personal Data relating to the individual data subject as set by Partner.

b) Logged Personal Data

Akamai processes Personal Data that is included in log files when performing the Services under the Channel Agreement ("Logged Personal Data"). Logged Personal Data is Personal Data logged by Akamai servers, relating to the access to Customer Content over the Akamai platform by Partner's or Partner's Clients' end users, as well as logged personal data associated with user activity and interaction with web and internet protocol sessions transiting Akamai's servers as part of a data subject's session with the Partner's or Partner's Clients' web property. Logged Personal Data include such data as:

a. End user IP addresses;

b. URLs of sites visited with time stamps (with an associated IP address);

c. Geographic location based upon IP address and location of Akamai server;

d. Telemetry data (e.g., mouse clicks, movement rates, and related browser data).

c) Site Personal Data

Akamai processes Personal Data associated with user activity and interaction with web and internet protocol sessions transiting Akamai's servers as part of a data subject's session with the Partner's or Partner's Clients' web property ("Site Personal Data"). The Site Personal Data consists of user telemetry

data (e.g., mouse clicks, movement rates, and user agent and related browser data) designed to measure website performance.

d) Enterprise Security Personal Data

Akamai processes Personal Data on behalf of customers of Akamai Enterprise Security Services that are provided by Partner's or Partner's Clients or collected during the provision of Services in order to protect users of the Partner's or Partner's Clients' enterprise network and the network itself from Internet security and policy abuse risks ("Enterprise Security Personal Data"). The Enterprise Security Personal Data includes such data as:

a. Login and user authentication data;

b. Contents of communications, including attachments;

c. Browser and device information, including location information;

d. URLs visited.

e) Special categories of data

Partner or Partner's Clients as the Data Controller decide which categories of data are included in the End User Personal Data. Where the Partner or Partner's Clients choose to include special categories of data in the Customer Content, Akamai will process this data as End User Personal Data, as instructed by the Partner or Partner's Clients.

4. Description of Akamai's Personal Data processing activities:

The following processing activities are performed when providing the Services:

a) End User Personal Data

Akamai processes End User Personal Data on behalf of Partner or Partner's Clients, including instructions given through the Channel Agreement, or via configuration of the Services via the relevant customer portals or support processes.

b) Logged Personal Data

Akamai collects Logged Personal Data and conducts analysis of Logged Personal Data to provide Partner with copies of traffic logs and data analytic reports related to the performance of the Services and the Partner's or Partner's Clients' web properties.

Logged Personal Data is also be processed for purposes of Service issue resolution.

c) Site Personal Data

Akamai processes Site Personal Data to provide website monitoring and analytics services to Partner or Partner's Clients to enable them to understand the nature of end user traffic to their web properties, as well as to monitor the performance of such properties.

d) Enterprise Security Personal Data

Akamai's Enterprise Security Services provides customers with tools and services to protect their employees and guests, as well as their network infrastructure from Internet threats. In addition, the same tools may be used to monitor network activity, provide secure access to applications, and establish and enforce access policies. To provide these Services, Akamai processes Enterprise Security Personal Data as needed to access and monitor network traffic, process and store access credentials and related network data as part of the network infrastructure services ordered by Partner.

Schedule 2 to the Data Processing Agreement
Akamai's Technical and Organizational Measures

Akamai's Technical and Organisational Measures to secure the Personal Data processed are publicly available in Akamai's Privacy Trust Center, https://www.akamai.com/us/en/multimedia/documents/akamai/technical-and-organizational-measures-to-secure-the-personal-data.pdf.