

DATA PROCESSING ADDENDUM

This data processing addendum (the "**Addendum**") amends the terms and forms part of the purchasing Agreement (the "**Agreement**") by and between you _____ (the "**Customer**") and Octopus Systems Ltd from which you are purchasing Octopus Cloud-Base Products (the "**Company**") and shall be effective on the later of (i) the effective date of the Agreement; or (ii) the date both parties execute this DPA in accordance with Section 1 below ("Effective Date"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

By entering into the Services Agreement, the Parties enter into this Addendum. For the purposes of this Addendum only, the term "Company" shall include Company and/or Company Affiliates, as the term Affiliate is defined below.

1. Instructions and Effectiveness:

- 1.1. This DPA has been pre-signed on behalf of Company. To enter into this DPA, Customer must:
 - a. Be a customer of the company Cloud-Base Products.
 - b. Complete the signature block below by signing and providing all relevant information; and
 - c. Submit the completed and signed DPA to the Company at Support@ocotpus-app.com
- 1.2. This DPA will only be effective (as of the Effective Date) if executed and submitted to the Company accurately and in full accordance with Section 1. Where Customer makes any deletions or other revisions to this DPA, this DPA will be null and void.
- 1.3. Customer signatory represents to the Company that he or she has the legal authority to bind Customer and is lawfully able to enter into this DPA
- 1.4. Notwithstanding expiry or termination of the Agreement, this DPA and any Standard Contractual Clauses (if applicable) will remain in effect until, and will terminate automatically upon, deletion by the Company of all personal data covered by this DPA, in accordance with this DPA.

2. Definitions

In this Addendum, the following words and phrases shall (unless the context otherwise requires) have the meanings set out beside them:

- 2.1. "**Agreement**" means the contract in place between Customer and in connection with the purchase of the Octopus Cloud-Base Products by Customer.

- 2.2. "**Applicable Laws**" shall mean European Union or a Member State law, Israeli Law, and any other applicable law with respect to any Company Personal Data, to which the Company is subject.
- 2.3. "**Applicable Privacy Laws**" shall mean EU Privacy Laws, the Israeli Data Protection Legislation, and, to the extent applicable, the data protection or privacy laws of any other country.
- 2.4. "**Customer Affiliate**" shall mean a person or entity controlling, controlled by or under the common control with the Customer; the term "control", for the purpose of this definition, shall mean direct or indirect possession of the power to direct or cause the direction of the management or policies of the Customer, whether through the ability to exercise voting power, by contract or otherwise.
- 2.5. "**Customer Data Subjects**" shall mean natural persons to which Customer Personal Data relate.
- 2.6. "**Customer Personal Data**" shall mean any Personal Data Processed by the Company or any Subcontractor pursuant to or in connection with the Services Agreement.
- 2.7. "**controller**", "**processor**", "**data subject**", "**personal data**" and "**processing**" (and "**process**") shall have the meanings given in European Data Protection Law; and shall also include "Owner" of a Database under the PPL.
- 2.8. "**EEA**" means the European Economic Area.
- 2.9. "**EU Privacy Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each EU member state and as amended, replaced or superseded from time to time, including by the GDPR and laws, rules and guidelines implementing or supplementing the GDPR.
- 2.10. "**GDPR**" shall mean 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 and repealing Directive 95/46/EC (General Data Protection Regulation), and as amended, replaced or superseded from time to time.
- 2.11. "**Israeli Data Protection Legislation**" shall mean the Israeli Privacy Protection Law ("PPL"), the regulations promulgated pursuant thereto and the applicable guidelines issued by the Privacy Protection Authority, and as amended, replaced or superseded from time to time.
- 2.12. "**Personal Data**" shall have collectively, the meaning ascribed to it in the GDPR and shall include "Data" and "Sensitive Data" as defined under the PPL.
- 2.13. "**Personal Data Breach**" shall mean a breach of security or other incident leading to the accidental or unlawful destruction, loss, alteration, the unauthorised disclosure or use of, or access to, or harm to the integrity of, Personal Data transmitted, stored or otherwise Processed.
- 2.14. "**End Users**" means an individual Customer permit or invite to use the Octopus Cloud-Base Products. For the avoidance of doubt: (a) individuals invited by Customer End Users, (b) individuals under managed accounts, and (c)

individuals interacting with an Octopus Cloud-Base Products as customer are also considered End Users

- 2.15. "**Processor**" shall have collectively, the meaning ascribed to it in the GDPR and shall also include "Holder" of a Database under the PPL.
- 2.16. "**Restricted Processing**" shall mean (1) the transferring of Customer Personal Data outside the EEA or to an International Organization, and (2) any Processing of Customer Personal Data that was transferred to any country outside the EEA or to an International Organization; in each case, where such transferring or Processing of Customer Personal Data would be prohibited by Applicable Privacy Laws in the absence of standard contractual clauses referred to in point (c) or (d) of Article 46(2) of the GDPR.
- 2.17. "**Subcontractor**" shall mean any person or entity appointed by or on behalf of Company to Process Customer Personal Data on behalf of the Customer in connection with the Services Agreement, excluding any employee of Company or of any such appointed person but including any Company Affiliate.
- 2.18. "**European Commission**", "**Data Subject**", "**International Organisation**", "**Member State**", and "**Processing**" shall have the meanings ascribed to them in the GDPR.
- 2.19. "**Database**", "**Database Manager**", "**Databases with Basic Security Level**", "**Databases with Medium Security Level**", "**Databases with High Security Level**", "**Information Security Officer**" and shall have the meanings ascribed to them in the Israeli Data Protection Legislation.

3. Authorization and Compliance

- 3.1. By virtue of the GDPR and the PPL, the Company is considered as the "Joint Controller" and "Processor" and the Customer is considered as the "Controller" with regards to the Customer and Customer's End Users Personal Data.
- 3.2. **EXHIBITS 3.2** to this Addendum sets out certain details regarding the Company's Processing of Customer Personal Data, as required by article 28(3) of the GDPR. Company may make reasonable changes to **EXHIBITS 3.2** as it considers necessary to meet those requirements.
- 3.3. Company shall comply with all Applicable Privacy Laws in the Controlling and Processing of Customer Personal Data.
- 3.4. Company shall not Process Customer Personal Data other than on documented instructions from the Customer and solely for the provision of the services under the Services Agreement and not for any other purpose, unless required to do so by Applicable Laws to which Company is subject, in which case Company shall inform Customer of that legal requirement before the relevant Processing, unless that Applicable Law prohibits such information on important grounds of public interest.
- 3.5. The Company warrants that in case Personal Data is collected directly by the Company's employees and/or Subcontractors, the collection shall be only by legal means under Applicable Laws, including but not limited to the use of legally registered Databases.

4. Company's Personnel

- 4.1. Company shall ensure that the access to Customer's Personal Data is strictly limited to those individuals who need to know or access the relevant Customer's Personal Data and as strictly necessary for the purpose of the Services Agreement.
- 4.2. Company is responsible to ensure that each individual who may have access to Customer Personal Data is subject to confidentiality undertakings or appropriate statutory obligations of confidentiality.
- 4.3. Company shall be responsible for any breach of this Addendum made by any of its employees, agents or contractors as if Company itself had made such breach.

5. Subcontractors

- 5.1. As of the date hereof, the Subcontractors engaged by Company are as set out in **Schedule 5.1**. Company declares that as of the date hereof, it has performed all the procedures set out in Article 5.3 below in respect of each such appointed Subcontractor.
- 5.2. Company shall inform Customer of any intended changes concerning the addition or replacement of a Subcontractor, by providing a minimum two months' advance written notice. Within two months of receiving such notice, Customer shall be entitled to notify Company in writing of any objections to the proposed changes ("**Customer Objection**"). In case of a Customer Objection, Company shall work with Customer in good faith to try settling out this issue. If the Parties fail to reach agreements within one month from the Customer Objection, notwithstanding anything in the Service Agreement, Customer may, at its sole discretion, terminate the Service Agreement or that part of the Service Agreement that requires the engagement of a Subcontractor, with immediate effect.
- 5.3. Subject to Article 5.2 above, before a Subcontractor first Processes Customer Personal Data, Company shall:
 - 5.3.1. Perform adequate due-diligence to ensure that Subcontractor is capable of providing the level of protection for Customer Personal Data required by any Applicable Privacy Law, the Services Agreement and this Addendum; and
 - 5.3.2. Ensure that the arrangement between the Company and the Subcontractor is regulated by a written agreement or other written instrument governed by EU Member State law/Israeli Applicable Law, imposing on the Subcontractor undertakings that guarantee at least the same level of protection for Customer Personal Data as those set out in this Addendum and meet the requirements of any Applicable Privacy Laws, including Articles 28(3) and 28(4) of the GDPR and Israeli Data Protection Legislation.
- 5.4. Company is responsible to ensure that each Subcontractor complies with the obligations under Articles 3.3, 3.4, 4, 6.1, 7, 8, 9, 11, 12, 13 and 14 of this Addendum as if it was party to this Addendum.

6. Customer Data Subjects' Rights

- 6.1. Company acknowledges the rights of Customer Data Subjects under the Applicable Privacy Laws, including those laid down in Chapter III of the GDPR (rights of the data subject) (e.g. access, modify, use or delete) and undertakes to assist the Customer by appropriate technical and organisational measures, for the fulfilment of the Customer's obligations to respond and, at no later than thirty (30) days from a given written request of the Customer, comply with or respond to requests for exercising Customer Data Subjects' rights as mentioned.
- 6.2. Without derogating from the generality of the above, Company shall (i) promptly notify Customer of any request raised by a Customer's Data Subject in relation to Customer Personal Data concerning him or her to Company and/or a Subcontractor; (ii) ensure that neither it nor any Subcontractor responds to any such request, except on a written instruction of the Customer or as required by Applicable Law to which the Company or the Subcontractor is subject, while in the latter case, unless that Applicable Law prohibits so, the Company shall inform, and if applicable, procure that the relevant Subcontractor informs the Customer of that legal requirement prior to responding to the request.

7. Personal Data Breaches

- 7.1. Immediately upon becoming aware of any Personal Data Breach affecting Customer Personal Data and, in any event, not later than 24 hours after becoming aware of that breach, Company shall (i) notify Customer of the breach; and (ii) provide Customer with all information necessary for the Customer to meet its obligations under Applicable Privacy Laws to notify the relevant public authorities of that Personal Data Breach and communicate it to Company Data Subjects if required.
- 7.2. Without derogating from the generality of the above, the information to be provided to Customer by Company pursuant to Article 7.1 above shall include, without limitation, (i) a description of the nature of the Personal Data Breach; (ii) the categories and numbers of Company Data Subjects concerned, and the categories and numbers of Company Personal Data records concerned; (iii) name and contact details of Contractor's, and if relevant, Subcontractor's, data protection officer and other contact point(s) where other information can be obtained; (iv) a description of the likely consequences of the Personal Data Breach; and (v) a description of the measures taken or proposed to be taken to address the Personal Data Breach, including measures to mitigate its possible adverse effects.
- 7.3. Where it is not possible to provide the above information at the same time, the information may be provided in phases, without undue further delays.
- 7.4. In any case where the Company delays in providing any information regarding a Personal Data Breach affecting Customer Personal Data to the Customer as provided above, the information shall be provided together with reasons for the delay.

- 7.5. Company shall cooperate with Customer in all reasonable and lawful efforts to prevent, mitigate or rectify such Personal Data Breach and promptly take all necessary steps and corrective actions required by Customer to investigate and handle any Personal Data Breach affecting Customer Personal Data.
- 7.6. Company shall document any Personal Data Breach affecting Customer Personal Data (including the facts relating to the Personal Data Breach, its effects and the remedial actions taken) in a sufficient manner to enable Customer to demonstrate compliance with any Applicable Privacy Law, including Article 33 of the GDPR and the PPL.
- 7.7. For avoidance of doubts, Customer, at its sole discretion, shall determine whether, when and what information to notify any Customer Data Subjects or data protection authorities regarding a Personal Data Breach. Except to the extent prohibited by applicable legal, regulatory or law enforcement requirements, Company must inform Customer prior to the publication or communication of any filings, communications, notices, press releases or reports related to any Personal Data Breach that expressly mention Customer or Customer 's Affiliates.

8. Data Security

- 8.1. Company shall, in relation to Customer Personal Data, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of varying likelihood and severity for the rights and freedoms of natural persons, including, as appropriate, the measures specified in Article 32(1) of the GDPR.
- 8.2. In assessing the appropriate level of security, Company shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

9. Restricted Processing

Notwithstanding anything to the contrary in the Services Agreement and/or this Addendum, the Company shall not, and procure that no Subcontractor shall, perform any Restricted Processing of any Customer Personal Data without the prior explicit written confirmation of the Customer.

10. Restricted transfers

The parties agree that when the transfer of Customer Personal Data is a Restricted Transfer and Applicable Data Protection Law requires that appropriate safeguards are put in place, it shall be subject to the appropriate Standard Contractual Clauses, which shall be deemed incorporated into and form a part of this DPA.

- 10.1. In relation to transfers of Customer Personal Data protected by the UK GDPR, the EU, SCCs will also apply in accordance, with the following modifications:
 - a) Any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the UK GDPR;

references to specific Articles of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK GDPR.

- b) References to "EU", "Union" and "Member State law" are all replaced with "UK"; Clause 13(a) and Part C of Annex I of the EU SCCs are not used; references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the Information Commissioner and the courts of England and Wales
- c) Clause 17 of the EU SCCs is replaced to state that "The Clauses are governed by the laws of England and Wales" and Clause 18 of the EU SCCs is replaced to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceeding against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts"

unless the EU SCCs, implemented as described above, cannot be used to lawfully transfer such Customer Personal Data in compliance with the UK GDPR in which case the UK SCCs shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes or Appendices of the UK SCCs shall be populated using the information contained in EXHIBITS A and B of this DPA (as applicable);

10.2. In relation to transfers of Customer Personal Data protected by the Swiss DPA, the EU SCCs will also apply in accordance with the following modifications:

- a) Any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA
- b) References to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as the case may be; and
- c) References to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the Swiss Federal Data Protection and Information Commissioner and competent courts in Switzerland

unless the EU SCCs, implemented as described above, cannot be used to lawfully transfer such Customer Personal Data in compliance with the Swiss DPA in which case the Swiss SCCS shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes or Appendices of the Swiss SCCs shall be populated using the information contained in EXHIBITS A and B to this DPA (as applicable);

11. Data Protection Impact Assessment (DPIA), Transfer Impact Assessment (TIA) and Prior Consultation

Company shall assist Customer with any assessment of the impact of the envisaged Processing operations on the protection of Customer Personal Data and prior consultations with data protection authorities, which Company considers to be required by it according to any Applicable Privacy Law, particularly Articles 35 and 36 of the GDPR.

12. Records

- 12.1. The Company, as well as (if applicable) any Subcontractor, shall maintain a written record of all categories of Processing activities carried out on behalf of the Customer, containing: (a) the name and contact details of the Customer, the Customer's representative and its data protection officer; (b) the categories of Processing carried out on behalf of the Customer; and (c) a general description of the technical and organizational security measures referred to in Article 8 above.
- 12.2. Immediately upon the request of the Customer and/or the relevant public authorities, Company shall make the records referred to in Article 12.1 above available to the Customer and/or relevant authorities (as required by Customer).
- 12.3. The Company will provide the Customer a written report on an annual basis, in sufficient detail, pertaining to its compliance to the Applicable privacy Laws in the performance of the services to the Customer.

13. Deletion or Return of Company Personal Data

- 13.1. Subject to Article 13.2, upon a written request of the Customer at any time and upon the termination of the Services Agreement for any reason whatsoever (each a "**Termination Event**"), the Company shall, at the Customer's option, promptly (i) permanently delete all Customer Personal Data in its possession or control such that the Customer Personal Data cannot be retrieved or reproduced, along with all copies, extracts and other objects or items in which it may be contained or embodied including any back-ups; or (ii) return to Customer by secure file transfer in such format as requested by Customer all Customer Personal Data in its possession or control and delete all such Customer Personal Data, along with all copies, extracts and other objects or items in which it may be contained or embodied.
- 13.2. The obligations of Company to delete Customer Personal Data pursuant to Article 13.1 above shall be subject to any obligations of Company under Applicable Laws requiring the storage of Customer Personal Data; *provided, however*, that Company shall (i) only retain such Customer Personal Data to the extent and for such period as required by such Applicable Laws; and (ii) ensure the confidentiality of all such Customer Personal Data and that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

- 13.3. Company shall provide written certification to Customer that it complied with the provisions of this Article 13 above within 7 (seven) days of the occurrence of a Termination Event.

14. Information and Audit Rights

Company shall make available to the Customer in a format as required under Applicable Privacy Laws all information necessary to demonstrate compliance with this Addendum and any Applicable Privacy Law and allow for and contribute to audits performed by Customer or an auditor mandated by Customer on Company's records and procedures, including at Company's facilities.

15. Requirements by Israeli Governmental Authorities

- 15.1. Company undertakes to appoint an Information Security Officer in accordance with section 17(b) of the PPL, even if it does not hold five or more databases. The information security officer shall be a person who's training and professional experience enables him to carry out such function as required.
- 15.2. Each party shall obtain and maintain all appropriate registrations if and to the extent required under the Israeli Data Protection Legislation in order to allow that party to perform its obligations under the Service Agreement. The Company will cooperate and provide the Customer with the relevant information required in order to register and report the Company (and/or any of the Company's Subcontractors) as a "Holder of Database" with the Israeli Registrar.
- 15.3. To the extent applicable to Company as a Database Holder, Company will use commercially reasonable efforts to comply with the binding instructions, orders and requirements, as conveyed by Customer, of Israeli governmental authorities, including, but not limited the Privacy Protection Authority, with respect to the Customer Personal Data ("Regulator Instructions"). Notwithstanding the foregoing, in the event Company is not able to comply with such Regulator Instructions, then Customer may terminate the Services Agreement by a thirty (30) day notice and all pre-paid fees will be refunded.

16. Miscellaneous



- 16.1. Nothing in this Addendum reduces the Company's obligations under the Services Agreement or Applicable Privacy Laws in relation to the protection of Customer Personal Data or permits Company to Process (or permit the Processing of) Customer Personal Data in a manner which is not explicitly authorized by the Services Agreement.
- 16.2. Subject to the provisions of Article 16.1 above, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the Parties, including the Services Agreement, the provisions of this Addendum shall prevail.

- 16.3. It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict;
- 16.4. The Customer may, by written notice to Company, propose changes to this Addendum which Customer reasonably considers to be necessary to comply with any Applicable Privacy Law; upon receipt of Customer's notice as mentioned, the Parties shall discuss and negotiate the proposed changes in good faith with the aim to achieve and ensure compliance with Applicable Privacy Laws and Company shall procure that changes corresponding to the agreed changes are made to the agreements or other written instruments entered into or executed in accordance with Article 5.3.2 above; *provided, however*, that if the Customer and Company do not reach an agreement as to the proposed changes, Customer has the right to terminate this agreement within 30 (thirty) days from the date in which the Customer notifies the Company of such proposed changes.
- 16.5. If any provision of this Addendum is held by a court of competent jurisdiction to be unenforceable under Applicable Law, then such provision shall be excluded from this Addendum and the remainder of this Addendum shall be interpreted as if such provision was so excluded and shall be enforceable in accordance with its terms; *provided, however*, that in such event this Addendum shall be interpreted so as to give effect, to the greatest extent consistent with and permitted by applicable law, to the meaning and intention of the excluded provision as determined by such court of competent jurisdiction.
- 16.6. Any notice or other document to be given under this Addendum shall be in writing and shall be deemed to have been duly given if sent via email, delivered by hand or sent by recorded delivery to the other Party at the address noted in the Services Agreement. Any such notice or other documents shall be deemed to have been received by the addressee 7 (seven) days following the date of dispatch if the notice or other document is sent by registered post, or in the following business day after the day in which the notice is received by personal delivery or sent via email.
- 16.7. This Addendum may be executed in one or more counterparts, each of which shall be deemed an original but all of which together shall constitute one and the same instrument.

IN WITNESS WHEREOF, the duly authorized representatives of both Parties have signed this Addendum

Octopus systems Ltd

Customer

Baruch Tagori - DPO	
Tal Bar Or - CEO	

May 22nd, 2022

OCTOPUS
control and command
514911494

EXHIBITS 3.2

Details regarding the Company's Processing of Customer Personal Data required by Article 28(3) of the GDPR

	<u>Data Exporter</u>	<u>Data Importer</u>
Name	a) Octopus systems Ltd b) Customer: _____	a) Octopus systems Ltd
Email Address	a) Support@octopus-app.com b) _____	a) Support@octopus-app.com
<u>Contact Person/ DPO</u>	a) Baruch Tagori	a) Baruch Tagori
<u>Contact Person/ _____</u>	c) Customer: _____	

Annex A(1) Description of Processing / Transfer:

The parties acknowledge that Company's processing of personal data will include all personal data submitted or uploaded to the Octopus Cloud-Base services by Customer and Customer's End Users from time to time, for the purpose of, or otherwise in connection with, Company providing the Services to Customer. Set out below are descriptions of the processing/transfers of personal data as contemplated as of the date of this DPA. Such descriptions are subject to change or may be supplemented pursuant to Section 2.3 of the DPA

Subject matter and duration of the Processing of Company Personal Data:

The subject matter and duration of the Processing of the Customer Personal Data are set out in the Services Agreement.

The nature and purpose of the Processing of Customer Personal Data:

The nature and purpose of the Processing of the Customer Personal Data are set out in the Services Agreement.

The types of Customer Personal Data to be Processed:

1		5		9	
2		6		10	
3		7		11	
4		8		12	

The categories of Data Subjects to whom the Customer Personal Data relates:

1		5		9	
2		6		10	
3		7		11	
4		8		12	

The obligations and rights of Customer:

The obligations and rights of Customer are set out in the Services Agreement and this Addendum.

EXHIBITS 5.1

Subcontractors

1	Microsoft Azure	2	Cloudflare	3	
---	-----------------	---	------------	---	--