ORCA SECURITY LICENSE AGREEMENT

This Agreement (the "**Agreement**") is entered into on the date of acceptance of the Order Form (as defined below) (the "**Effective Date**"), by and between the relevant Orca Security entity according to Section 17below and its affiliates (the "**Company**") and the entity accepting the Order Form (the "**Customer**") (each, a "**Party**" and collectively, the "**Parties**"). Customer may use the Products (as defined below), subject to the following terms:

1. **License.** Subject to the terms and conditions of this Agreement, Company hereby grants Customer a limited, non-exclusive, non-sublicensable, non-assignable, non-transferable and revocable license to: (i) remotely access and use (i.e., on a SaaS basis) Company's software as a service known as "Orca Cloud Security Platform" (the "**Platform**"); (ii) if so indicated in the applicable Order Form (defined below), to install and use the software agents in object code form (the "**Sensors**"); and (iii) if so indicated in the applicable Order Form, to install and use the Company's application security software in object code form (the "**Orca AppSec"**), and use them as well as any documentation (**"Documentation**") related thereof for internal business purposes. The Platform, Sensors, and Orca AppSec shall be referred to as the "**Products**". Customer may only use the Products in accordance with the Documentation, subject to the use limitations indicated in an order form or purchase order: (a) signed by the Parties; or (b) approved in writing by Company and provided by Company's authorized partner (**"Order Form**") and applicable laws.

2. **Services.** In addition to the abovementioned licenses, if applicable, Company may provide services, as detailed in a Statement of Work negotiated and signed by the Parties. Support and maintenance services are provided according to the Service Level Agreement attached hereto as Exhibit A ("**SLA"** and collectively with the Products, the "**Services"**).

3. **Payment.** The Services are conditioned on Customer's payment in full of the applicable fees set forth in the Order Form. Company shall not be bound by any additional or conflicting terms set forth in any purchase order or sales acknowledgement submitted by the Customer. To the extent Customer purchases a subscription directly from Company, unless otherwise specified in the Order Form: (i) Customer will pay all amounts due under this Agreement in U.S. Dollars currency; and (ii) all amounts invoiced hereunder are due and payable within thirty (30) days of the date of the invoice. If any payment under this Agreement is not made on or before the due date, Customer shall pay interest on the overdue amount at the rate of 1.5% per month (compounded daily) from the due date until the date of payment, or the highest interest possible subject to applicable law. All amounts payable under this Agreement are exclusive of all excises, sales, use, gross-turnover, value-added, withholding, goods and services tax and other direct or indirect taxes, charges, levies and duties, but excluding Company's net income taxes ("**Indirect Taxes**") and Customer will be liable for reporting and payment of such Indirect Taxes in its tax jurisdiction including, without limitation, any required self-invoices (if applicable). During the Term, If Customer's use of the Products exceeds Customer's subscription's usage limits, Company shall perform a true-up (if applicable, via Company's authorized partner) and invoice Customer for the excess use, at a price per unit according to the Order Form.

4. **Customer Account**. The Products may only be used through a customer account (the "**Account**"). Such Account may be accessed solely by Customer's employees or service providers who are explicitly authorized by Customer to use the Products (each, a "**Permitted User**"). Customer will ensure that the Permitted Users keep the Account login details secure at all times and comply with the terms of this Agreement; and will be fully responsible for any breach of this Agreement by a Permitted User. Unauthorized access or use of the Account or the Products must be immediately reported to the Company. Customer acknowledges and agrees that Company does not monitor or control Customer's cloud environment or configurations.

5. **Prohibited Uses.** Except as specifically permitted herein, without the prior written consent of the Company, Customer must not, and shall not allow any Permitted User or any third party to, directly or indirectly: (i) copy, modify, create derivative works of or distribute any part of the Products (including by incorporation into its products), or use any of the intellectual property related to the Products to create any computer program or other material that performs, replicates, or utilizes the same or substantially similar functions as the Products; (ii) sell, license (or sub-license), lease, assign, transfer, pledge, or share Customer's rights under this Agreement with any third party; (iii) use any "open source" or "copyleft software" in a manner that would require the Company to disclose the source code of the Products to any third party; (iv) disassemble, decompile, reverse engineer or attempt to discover the Products' source code or underlying algorithms; (v) use the Products in a manner that violates or infringes any rights of any third party, including but not limited to, privacy rights, publicity rights or intellectual property rights; (vi) remove or alter any trademarks or other proprietary notices related to the Products; (vii) circumvent, disable or otherwise interfere with security-related features of the Products or features that enforce use limitations; (viii) export, make available or use the Products in any manner prohibited by applicable laws (including without limitation export control laws); and/or (ix) transmit any malicious code (i.e., software viruses, Trojan horses, worms, malware, or other computer instructions, devices, or techniques that erase data or programming, infect, disrupt, damage, disable, or shut down a computer system or any component of such computer system), perform or permit any intrusive, disruptive, or unauthorized security testing (including penetration testing, vulnerability assessments, or similar tests), or otherwise use the Products in any manner that interferes with, degrades, or disables any functionality or security feature of the Products. Any permitted security testing shall only be conducted subject to Company's written confirmation and in accordance with Company's VDP Policy.

6. **Customer Data and Usage Data**. As part of the Services, the Platform receives a read-only view of the Customer's cloud environment, which is then assessed by a virtual scanner for various security risks. The results are presented through the Customer dashboard within the Platform as 'alerts' (collectively, the "**Reports**"). Customer shall be deemed the exclusive owner of the Reports. Customer shall retain all rights, titles, and interests in and to all non-public data provided by

Customer to Company in connection with the Services ("**Customer Data**"). Customer represents that it has the right and authority to and has obtained all necessary consents required to use and provide Customer Data for the purposes described herein. Company may process information, including, without limitation, login information, system integrations, API usage information, and information regarding Customer's use of the Products ("**Usage Data**"), for customer success, customer satisfaction and support purposes. Additionally, to provide the Services and for Customer to benefit from the Products' capabilities applicable to Customer's environment in full, Company's employees may access Customer's Platform dashboard and production environment.

7. **Mutual Warranties**. Each Party represents and warrants that it is duly organized, validly existing and in good standing under the laws of its jurisdiction of incorporation or organization; and that the execution and performance of this Agreement will not conflict with other agreements to which it is bound or violate applicable law and each Party shall comply with all applicable privacy laws.

8. **Intellectual Property Rights.** The Products are not for sale and are solely the Company's and/or its licensors' property. All rights, titles, and interests, including any intellectual property rights evidenced by or embodied in, attached, connected, and/or related to the Products and any and all improvements and derivative works thereof are and shall remain owned solely by the Company and/or its licensors, as applicable. This Agreement does not convey to Customer any interest in or to the Products other than a limited right to use the Products in accordance with Section 1. Nothing herein constitutes a waiver of the Company's intellectual property rights under any law.

If Company receives any feedback (*e.g.*, questions, comments, suggestions or the like) regarding the Products and/or Services hereunder (collectively, "**Feedback**"), all rights, including intellectual property rights in such Feedback shall belong exclusively to Company and such shall be considered Company's Confidential Information and Customer hereby irrevocably and unconditionally transfers and assigns to Company all intellectual property rights it has in such Feedback and waives any and all moral rights that Customer may have in respect thereto. It is further understood that the use of Feedback, if any, may be made by Company at its sole discretion, and that Company in no way shall be obliged to make use of any kind of the Feedback or part thereof.

9. **Third Party Components**. The Products may use or include third party software, files, libraries or components that are subject to third party open-source license terms ("**Open-Source Licenses**"). The respective licenses or notices of such Open-Source Licenses are available within the Platform and may be updated from time to time.

10. **Integrations**. The Products may contain features designed to interoperate with third party applications and services that are not owned or related to Company ("**Non-Orca App**"). Subject to Customer's approval, Customer may connect the Account to a Non-Orca App which will allow the exchange of data between Company and the Non-Orca App, including without limitation, the Reports, the scope of which is determined by the applicable actions set by such integration. Customer hereby acknowledges that any access, collection, transmission, processing, storage or any other use of data, including the Reports, by a Non-Orca App, is governed by a separate agreement between Customer and the licensor of the Non-Orca App, including any applicable privacy policy, and Company is not responsible for any act or omission of such third party. Company cannot guarantee the continued availability, security and interoperability of Non-Orca Apps and may cease providing them without entitling Customer to any compensation, if for example and without limitation, the provider of a Non-Orca App ceases to make the Non-Orca App available for interoperation with the corresponding Service features in a manner acceptable to Company.

11. **Confidentiality**. Each Party may have access to certain non-public and/or proprietary information of the other Party, in any form or media, including without limitation trade secrets and other information related to the products, software, technology, data, know-how, or business of the other Party, and any other information that a reasonable person should have reason to believe is proprietary, confidential, or competitively sensitive (the "**Confidential Information**"). The Documentation shall also be considered as Confidential Information hereunder. Each Party shall take reasonable measures, at least as protective as those taken to protect its own confidential information, but in no event less than reasonable care, to protect the other Party's Confidential Information from disclosure to a third party. The receiving party's obligations under this Section, with respect to any Confidential Information of the disclosing party, shall not apply to and/or shall terminate if such information: (a) was already lawfully known to the receiving party at the time of disclosure by the disclosing party; (b) was disclosed to the receiving party by a third party who had the right to make such disclosure without any confidentiality restrictions; (c) is, or through no fault of the receiving party has become, generally available to the public; or (d) was independently developed by the receiving party without access to, or use of, the disclosing party's Confidential Information. Neither Party shall use or disclose the Confidential Information of the other Party except for the performance of its obligations under this Agreement ("**Permitted Use**"). The receiving party shall only permit access to the disclosing party's Confidential Information to its respective employees, consultants, affiliates, agents and subcontractors having a need to know such information in connection with the Permitted Use, who either (i) have signed a non-disclosure agreement with the receiving party containing terms at least as restrictive as those contained herein or (ii) are otherwise bound by a duty of confidentiality to the receiving party at least as restrictive as the terms set forth herein. The receiving party will be allowed to disclose Confidential Information to the extent that such disclosure is required by law or by the order or a court of similar judicial or administrative body, provided that it notifies the disclosing Party of such required disclosure to enable disclosing party to seek a protective order or otherwise prevent or restrict such disclosure. All rights, titles, and interests in and to Confidential Information are and shall remain the sole and exclusive property of the disclosing Party. Nothing contained herein will require the destruction or purging of Confidential Information maintained on routine computer system

backup tapes, disks or similar storage devices.

12. **LIMITED WARRANTIES.** The Company represents and warrants that, under normal authorized use, the Products shall substantially perform in conformance with its Documentation. If the Products fail to conform to the foregoing warranty, Customer's sole remedy is for Company to repair the Products. If Company does not correct a substantial non-performance within thirty (30) days following notice to Company thereof, then Customer may terminate this Agreement pursuant to Section **Error! Reference source not found.**. The warranty set forth shall not apply if the failure of the Products results from or is otherwise attributable to: (i) repair, maintenance or modification of the Products by persons other than the Company or its authorized contractors; (ii) accident, negligence, abuse or misuse of the Products by Customer; (iii) use of the Products by Customer other than in accordance with the Documentation; (iv) Customer's failure to implement software updates provided by the Company specifically to avoid such failure; or (v) the combination of the Products with equipment or software not authorized or provided by the Company; or (vi) Customer's failure to properly maintain its computing environment used to access the Services. OTHER THAN AS EXPLICITLY STATED IN THIS AGREEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, THE SERVICES AND/OR THE REPORTS ARE PROVIDED ON AN "AS IS" BASIS. THE COMPANY AND/OR ITS LICENSORS DO NOT WARRANT THAT THE SERVICES OR REPORTS: (I) WILL MEET CUSTOMER'S REQUIREMENTS; (II) WILL BE UNINTERRUPTED OR ERROR-FREE; OR (III) WILL PROTECT AGAINST ALL POSSIBLE THREATS WHETHER KNOWN OR UNKNOWN. COMPANY DOES NOT ASSUME ANY LIABILITY WITH RESPECT TO CUSTOMER'S CLOUD ENVIRONMENT'S SECURITY, COMPLIANCE, RESOURCE UTILIZATION AND COST. EXCEPT AS SET FORTH IN SECTION 7 (*MUTUAL WARRANTIES*) AND THIS SECTION 12 (*LIMITED WARRANTIES*), THE COMPANY EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING MERCHANTABILITY, TITLE, NON-INTERFERENCE, AND FITNESS FOR A PARTICULAR PURPOSE.

13. **LIMITATION OF LIABILITY**. EXCEPT FOR ANY DAMAGES RESULTING FROM ANY BREACH OF EITHER PARTY'S CONFIDENTIALITY OBLIGATIONS HEREIN; EITHER PARTY'S WILLFUL MISCONDUCT, FRAUD AND/OR CUSTOMER'S MISAPPROPRIATION OR OTHERWISE VIOLATION OF COMPANY'S INTELLECTUAL PROPERTY RIGHTS (INCLUDING MISUSE OF THE LICENSE BY CUSTOMER PURSUANT TO SECTION 1); NEITHER PARTY AND/OR ITS LICENSORS SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR ANY LOSS OF REVENUE, REPUTATION, OR PROFITS, DATA, OR DATA USE.

EXCEPT FOR ANY DAMAGES RESULTING FROM ANY BREACH OF EITHER PARTY'S CONFIDENTIALITY OBLIGATIONS HEREIN; A PARTY'S WILLFUL MISCONDUCT, FRAUD, AND/OR DAMAGES RESULTING FROM CUSTOMER'S MISAPPROPRIATION OR OTHERWISE VIOLATION OF COMPANY'S INTELLECTUAL PROPERTY RIGHTS (INCLUDING MISUSE OF THE LICENSE BY CUSTOMER PURSUANT TO SECTION 1); EITHER PARTY'S AND/OR ITS LICENSORS' MAXIMUM LIABILITY FOR ANY DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER IN CONTRACT OR TORT, OR OTHERWISE, SHALL IN NO EVENT EXCEED, IN THE AGGREGATE, THE TOTAL AMOUNTS ACTUALLY PAID TO COMPANY IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH CLAIM. THIS LIMITATION OF LIABILITY IS CUMULATIVE AND NOT PER INCIDENT.

14. **Indemnification**.

A. **Indemnification By Company**. Company acknowledges and agrees to defend, at its expense, any third party action or suit brought against the Customer alleging that the Products, when used as permitted under these TOS, infringes intellectual property rights of a third party (**"IP Infringement Claim"**); and the Company will pay any damages awarded in a final judgment against the Customer that are attributable to any such claim. If the Products (or any part thereof) become, or in the Company's opinion is likely to become, the subject of an IP Infringement Claim, then the Company may, at its sole discretion: (a) procure for the Customer the right to continue using the Products; (b) replace or modify the Products to avoid the IP Infringement Claim; or (c) if options (a) and (b) cannot be accomplished despite the Company's reasonable efforts, then the Company may terminate this Agreement and in such event discontinue the use of the affected Products (or any part thereof) and provide a refund for any amount pre-paid by Customer for the use of the Products (or any part thereof) with respect to the remaining unused period of the license. Notwithstanding the foregoing**,** the Company shall have no responsibility for IP Infringement Claims resulting from or based on: (i) use of the Products is in violation of this Agreement or, in a material respect, not in accordance with the Documentation; (ii) modifications to the Products made by a party other than the Company or its designee; (iii) the Customer's failure to implement software updates provided by the Company specifically to avoid infringement or where Customer continues the allegedly infringing activity after being notified; or (iv) combination or use of the Products with equipment, devices or software not supplied by the Company or not in accordance with the Documentation. This Section states Company's entire liability, and Customer's exclusive remedy, for claims or alleged or actual infringement.

B. **Indemnification By Customer**. Customer acknowledges and agrees to defend, at its expense, any third party action or suit brought against the Company alleging that Company's and/or its licensors' use of the Customer Data as permitted under this Agreement, infringe any rights of a third party; and the Customer will pay any damages awarded in a final judgment against the Company that are attributable to any such claim.

C. **Indemnification Procedures.** The indemnifications outlined above are contingent upon the following

conditions: (i) The indemnified party promptly notifies the indemnifying party in writing of any such claims; (ii) The indemnified party grants the indemnifying party exclusive authority to manage the defense or settlement of said claims, and offers all reasonable information and assistance at the indemnifying party's expense; and (iii) The indemnified party refrains from making any admissions that could impact the indemnifying party's defense. The indemnifying party will not be bound by any settlement that the indemnified party enters into without the indemnifying party's prior written consent.

15. **Privacy.** To the extent that Customer needs a data processing agreement, Customer and Company shall enter into the Data Processing Agreement attached as **Exhibit B ("DPA")**.

16. **Term and Termination.** This Agreement shall enter into force and effect on the Effective Date and shall remain in full force as long as there is an Order Form in effect (collectively, the "**Term"**). If there is no Order Form in effect for a period of ninety (90) days, this Agreement will terminate automatically. Company shall have the right to immediately suspend without notice any or all related Services provided to Customer hereunder, in the event Customer (i) fails to pay Company any amounts past due, or (ii) is in breach of Section 5 (*Prohibited Uses*). In addition, either Party may terminate this Agreement with immediate effect if the other Party materially breaches this Agreement and such breach remains uncured fifteen (15) days after having received written notice thereof. Company may immediately terminate this Agreement upon written notice in the event that Company reasonably believes, subject to credible evidence, the Customer has violated any of the Trade Controls (as defined below) and such violation cannot be promptly corrected to Company's reasonable satisfaction despite commercially reasonable measures or is incurable as a matter of law or if Customer becomes designated as a prohibited party under the Trade Controls or becomes owned 50 percent or more, or otherwise controlled, by such parties; or is designated as a party for which authorization is required for it to continue use the Products and Services under this Agreement. Upon termination or expiration of this Agreement: (i) the Products licenses granted to Customer under this Agreement shall expire, and Customer shall discontinue any further use and access thereof (including deletion of the Sensors and Orca AppSec from Customer's systems); (ii) Customer shall immediately delete and dispose of all copies of the Documentation in Customer's or any of its representatives' possession or control; (iii) Company shall delete the Reports**;** and (iv) Customer shall not be relieved of its duty to discharge in full all due sums owed by Customer to Company under this Agreement until the date of termination or expiration hereof. The following sections shall survive termination of this Agreement: Section **Error! Reference source not found.**3 (*Payment*) with respect to payable fees, Section **Error! Reference source not found.**5 (*Prohibited Uses*), Section 8 (*Intellectual Property Rights*), Section 11 (*Confidentiality*), Section 13 (*Limitation of Liability*), Section 16 (*Term and Termination*), Section **Error! Reference source not found.**19 (*Governing Law and Jurisdiction*), Section 20 (*Miscellaneous*). Customer shall be responsible for downloading its Reports prior to termination of this Agreement. The termination of this Agreement shall not limit either Party from pursuing any other remedies available to it under applicable law.

17. **Orca Entities.** The relevant Orca Security entity engaging hereunder shall be as follows:

Customer's Locations	**Relevant Orca Security Entity**
A. If Customer is located in the territory of the Americas	Orca Security Inc. with a principal place of business at: 1455 NW Irving St., Suite 390 Portland, OR 97209
B. If Customer is located in the territory of the UK	Orca Security UK Ltd. with a principal place of business at: C/O Lakin Rose Limited Pione, Vision Park, Histon, Cambridge CB24 9NL, United Kingdom.
C. If Customer is located in the territory of Australia	Orca Security Australia Pty Ltd. with a principal place of business at: Mazars (NSW) Pty Limited, Level 12, 90 Arthur Street, North Sydney NSW 2060
D. Otherwise, If Customer is not located in A, B or C above	Orca Security Ltd. with a principal place of business at: 3 Tushia St., Tel Aviv, Israel 6721803

18. **Export Controls**. Customer agrees to comply with applicable export control and financial sanctions laws in connection with its use of the Company's Platform and Services, including, but not limited to, the United States Export Administration Regulations ("**EAR**") and the United States Foreign Assets Control Regulations ("**OFAC Regulations**") (collectively "**Trade Controls**"). Customer agrees it will not export, re-export or transfer in-country to, use for the benefit of, or permit access to the Platform and Services by: (1) any party that is currently in, a citizen of, ordinarily resident in, organized under the laws of, or owned or controlled by the government of, any country or region prohibited under the Trade Controls (as may be amended from time to time); or (2) any destination, party, or end use subject to license requirements imposed by the Trade Controls, including but not limited to destinations for which no general license or license exception is available (e.g., Russia and Belarus) or are limited or restricted by law, regulation or order administered by the United States, and any party owned (in whole or in part) by any such party or acting on behalf of any such party.

19. **Governing Law and Jurisdiction**. Any dispute that arises between the Parties relating to this Agreement, including the application, interpretation, implementation or validity of this Agreement, shall be finally resolved by binding arbitration in English, under Israeli law, before a sole arbitrator in Toronto, Canada under the ADR

Chambers Expedited Arbitration Rules and its Section 8 (In Writing Arbitration). The Parties agree that the ADR Chambers Expedited Arbitration Rules (and the application of section 8 thereof, requiring the parties to arbitrate In Writing Only) gives the Parties a fair opportunity to present their case and respond to the case of the other side, which opportunity is a cost-effective solution for disputes of this magnitude. Judgment upon the award rendered by the arbitrator appointed by ADR Chambers may be entered in any court having jurisdiction.

20. **Miscellaneous.** This Agreement - including any Order Forms, Statements of Work, and any exhibits attached or referred hereto - represents the complete agreement concerning the subject matter hereof and may be amended only by a written agreement executed by both Parties. In the event of any conflict or inconsistency within the Agreement, the order of precedence shall be: (1) the applicable Order Form or SOW, (2) this Agreement. The failure of either Party to enforce any rights granted hereunder or to take action against the other Party in the event of any breach hereunder shall not be deemed a waiver by that Party as to subsequent enforcement of rights or subsequent actions in the event of future breaches. If any provision of this Agreement is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. Any use of the Services by an agency, department, or other entity of the United States government shall be governed solely by the terms of this Agreement. Neither Party may assign its rights or obligations under this Agreement without the prior written consent of the other Party, which consent may not be unreasonably withheld or delayed, provided, however, that either Party may, upon notice to the other Party, assign its rights and obligations under this Agreement in connection with a merger, consolidation, or the sale of all or substantially all of the assets or business of such Party. The Agreement shall bind and inure to the benefit of the successors and permitted assigns of the respective parties. Any assignment or transfer not in accordance with this Agreement shall be void. Company may, in its reasonable discretion, use Customer's name and logo on its website and in its marketing materials as a reference customer. Media releases and public announcements or disclosures relating to this Agreement, its subject matter or the potential business transaction between the Parties shall be coordinated with and consented to by both Parties in writing prior to the release thereof. This Agreement does not, and shall not be construed to create any relationship, partnership, joint venture, employer-employee, agency, or franchisor-franchisee relationship between the Parties. Either Party will not be liable for any delay or failure to perform its obligations resulting from circumstances or causes beyond its reasonable control. This Agreement may be executed in electronic counterparts, each of which counterpart, when so executed and delivered, shall be deemed to be an original and all of which counterparts, taken together, shall constitute but one and the same agreement. All notices under this Agreement shall be deemed effective upon receipt and shall be in writing and (a) delivered personally, (b) sent by commercial courier with written verification of receipt, (c) sent by certified or registered U.S. mail, postage prepaid and return receipt requested, or (d) sent via electronic mail with read receipt requested, to the Party to be notified at the address and/or electronic address set forth hereinafter for such Party:

For Orca Security Attn: Legal, 3 Tushia St., Tel Aviv, Israel, 6721803 **Electronic Mail:** Legal@orca.security

* * * * * * * *

EXHIBIT A

SERVICE LEVEL AGREEMENT (SLA)

Company reserves the right to change the terms of this SLA by providing Customer with at least thirty (30) days prior written notice.

1. **Definitions**:

   - "**Cloud Provider**" means a third-party cloud computing platform on which the Company Service(s) are hosted, including, but not limited to, Google Cloud Platform (GCP), Amazon Web Services (AWS) and Microsoft Azure.
   - "**Downtime**" means the time in which the Platform is unavailable to the Customer, as measured and determined solely by Company based on its servers. Downtime shall exclude Regular Maintenance and Scheduled Maintenance.
   - "**Downtime Period**" means the total accumulated number of Downtime minutes in a calendar month.
   - "**Monthly Uptime Percentage**" means the total number of minutes in a calendar month, minus the Downtime Period, divided by the total number of minutes in a calendar month minus Exclusions (as defined below), and multiplied by one hundred (100).

$$\frac{[Total\ number\ of\ minutes\ in\ a\ calendar\ month] - [Downtime]}{[Total\ number\ of\ minutes\ in\ a\ calendar\ month] - [Exclusions]}\ X\ 100 = Monthly\ Uptime\ Percentage$$

   - "**Pro Rata Monthly Amount**" means the portion of the fees paid by the Customer in the applicable month in which the Downtime occurred and that are attributable to the Cloud Provider associated with the Downtime.
   - "**Regular Maintenance**" is the period under which the Platform may be unavailable for recurring maintenance work. Company shall conduct Regular Maintenance between the hours of 2AM and 6AM (EST) Saturday and Sunday.
   - "**Scheduled Maintenance**" is the period under which the Platform may be unavailable for non-recurring maintenance. Company shall provide customers subscribed to receive maintenance updates at least a twenty-four (24) hours advance notice prior to Scheduled Maintenance. Company shall use commercially reasonable efforts to minimize any Scheduled or Regular Maintenance windows to the minimum time necessary to support performance of the Services.
   - "**Service Credit**" means credit notes due to the Customer as a result of Downtime Period as detailed in the table below.

2. **Service Commitment**. During the term of the Agreement, Company will use commercially reasonable efforts to make the Platform available with a Monthly Uptime Percentage of at least 99.9% (the "**Service Commitment**"). In the event that Company does not meet the Service Commitment, the Customer will be eligible to receive Service Credits as described in the table below.

Monthly Uptime Percentage	**Service Credits**
Between 99.0% – 99.9% (inclusive)	5% of the applicable Pro Rata Monthly Amount
Less than 99.0%	10% of the applicable Pro Rata Monthly Amount

Service Credits Eligibility.

In order to receive any of the Service Credits described above, the Customer must (i) notify Company's technical support team within thirty (30) days from the end of the applicable month in which Customer becomes eligible to receive Service Credits; and (ii) submit Company's technical support team all information necessary for Company to validate the Customer's claim, including but not limited to, a detailed description of the Downtime incident, its time and duration. Failure to comply with these requirements will forfeit such Customer's right for Service Credits for such Downtime. In addition, the Customer must be in compliance with the Agreement in order to be eligible for a Service Credit.

Maximum Service Credits.

The aggregate maximum number of Service Credits to be issued by Company to the Customer for any and all Downtime Periods that occur in a single subscription period shall not exceed 10% of the amount due by Customer for the Company Services provided to it during the applicable subscription period.

The Service Credits will be issued as monetary credit applied against a future Order Form signed by the Parties. The Service Credits will not entitle the Customer to any refund or other payment from Company.

THE CUSTOMER HEREBY ACKNOWLEDGES AND AGREES THAT ITS RIGHT TO RECEIVE SERVICE CREDITS AS SPECIFIED ABOVE CONSTITUTES ITS SOLE AND EXCLUSIVE REMEDY FOR ANY DOWNTIME OR UNAVAILABILITY.

Sensor Support. Customer acknowledges and agrees that Company shall provide support with respect to Sensors for Versions up to two (2) months prior. If Customer is utilizing older Versions of the Sensor Customer acknowledges and understands that any support services associated with the Sensors may be limited or delayed. It is the Customer's responsibility to maintain updated Versions to benefit from the fullest extent of support services offered by Company.

"**Version**" means a distinct release, or iterations of the Sensor developed and made available to Customer by Company. Each Version is identified by a specific numerical or alphanumeric designation.

Exclusions. The following occurrences shall be considered as Exclusions under this SLA. Platform unavailability that is caused by: (a) factors beyond Company's reasonable control (e.g. any force majeure event, abnormal environmental conditions, electrical stress, internet access or related problems etc.); (b) results or outcomes attributable to repair, maintenance or modification of Company's Services by persons other than Company's authorized third parties; (c) use of the Company's Platform other than in accordance with its manuals, specifications or Documentation or in violation of the Agreement; (d) Customer's or third party's equipment, software or other technology (other than third party equipment within Company's direct control); and/or (e) Regular and Scheduled Maintenance. Furthermore, Company shall have no liability for Downtime regarding features or functionalities that are not intended for production use (e.g., beta testing).

EXHIBIT B

DATA PROCESSING AGREEMENT/ADDENDUM

This Data Processing Agreement ("**DPA**") is made and entered into as of the Effective Date of the Orca Security License Agreement (the "**Agreement**") between **Customer (or "Data Controller")** and **Company ("Orca", "Service Provider" or "Data Processor")** and reflects the parties' agreement with regard to the Processing of Personal Data (as such terms are defined below) of individuals. Both parties shall be referred to as the "**Parties**" and each, a "**Party**".

WHEREAS, Orca shall provide the services set forth in the Agreement (collectively, the "**Services**") for Customer, as described in the Agreement; and

WHEREAS, In the course of providing the Services pursuant to the Agreement, Orca may process Personal Data on Customer's behalf, in the capacity of a "Data Processor" and/or "Service Provider" to the extent the California Consumer Privacy Act (as may be amended from time to time) (the "**CCPA**") is applicable; and the Parties wish to set forth the arrangements concerning the processing of Personal Data (defined below) within the context of the Services and agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

NOW THEREFORE, in consideration of the mutual promises set forth herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged by the Parties, the parties, intending to be legally bound, agree as follows:

1. INTERPRETATION AND DEFINITIONS

1.1 The headings contained in this DPA are for convenience only and shall not be interpreted to limit or otherwise affect the provisions of this DPA.

1.2 References to clauses or sections are references to the clauses or sections of this DPA unless otherwise stated.

1.3 Words used in the singular include the plural and vice versa, as the context may require.

1.4 Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement.

1.5 Definitions:

(a) "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "**Control**", for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

(b) "**Authorized Affiliate**" means any of Customer's Affiliate(s) which: (a) is subject to the Data Protection Laws and Regulations, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Orca but has not signed its own agreement with Orca.

(c) **"Controller", "Data Controller" or "Business"** means the entity which determines the purposes and means of the Processing of Personal Data.

(d) **"Data Protection Laws and Regulations"** means U.S. Data Protection Laws and European Data Protection Laws that apply to the processing of Customer's Personal Data hereunder.

(e) **"Data Subject"** means the identified or identifiable natural person to whom the Personal Data relates.

(f) "**European Data Protection Laws**" means: (i) 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 (General Data Protection Regulation) (the "**GDPR**"); (ii) with respect of the United Kingdom, the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); and (iii) the EU e-Privacy Directive (Directive 2002/58/EC).

(g) **"Member State"** means a country that belongs to the European Union and/or the European Economic Area. "Union" means the European Union.

(h) "**Orca**" means the relevant Orca entity of the following Orca legal entities: Orca Security Ltd, Orca Security UK Ltd. and Orca Security Inc.

(i) **"Personal Data"** means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(j) **"Process(ing)"** means any operation or set of operations which is performed upon Personal Data in connection with the Services, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(k) **"Processor", "Data Processor" or "Service Provider"** means the entity which Processes Personal Data on behalf of the Controller.

(l) **"Security Documentation"** means the technical and organizational measures applicable to the specific Services purchased by Customer, as set forth in Annex 2.

(m) **"Sub-processor"** means any third-party processor engaged by Orca to perform Processing in connection with the Services.

(n) "**Supervisory Authority**" means government agency or law enforcement authority, including judicial authorities.

(o) "**U.S. Data Protection Laws**" means all data protection or privacy laws and regulations applicable to Customer's Personal Data within the United States, including the CCPA.

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties.** The Parties acknowledge and agree that with regard to the Processing of Personal Data, the Customer is the Controller of the Personal Data and Orca is the Processor of such data, except when the Customer acts as a Processor of the Personal Data, in which case Orca is a sub-processor.

2.2 **Customer's Processing of Personal Data.** Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations and comply at all times with the obligations applicable to Data Controllers. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the means by which Customer acquired Personal Data. Without limitation, Customer shall comply with any and all transparency-related obligations (including, without limitation, displaying any and all relevant and required privacy notices or policies) and shall have any and all required legal bases in order to collect, Process and transfer to Orca the Personal Data and to authorize the Processing by Orca of the Personal Data which is authorized in this DPA.

2.3 **Orca's Processing of Personal Data.**

2.3.1 Subject to the Agreement, Orca shall Process Personal Data in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and this DPA and to provide the Services; (ii) Processing for Customer to be able to use the Services; (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement; (iv) Processing as required by a Supervisory Authority to which Orca is subject; in such a case, Orca shall inform the Customer of the legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

2.3.2 To the extent that Orca cannot comply with a request from Customer and/or its authorized users relating to Processing of Personal Data (including, without limitation, any instruction, direction, code of conduct, certification, or change of any kind), Orca (i) shall inform Customer, providing relevant details of the problem (which shall not be considered legal advice), (ii) Orca may, without any kind of liability towards Customer, temporarily cease all Processing of the affected Personal Data (other than securely storing those data), and (iii) if the Parties do not agree on a resolution to the issue in question and the costs thereof, each Party may, as its sole remedy, terminate the Agreement and this DPA with respect to the affected Processing, and Customer shall pay to Orca

all the amounts owed to Orca or due before the date of termination. Customer will have no further claims against Orca (including, without limitation, requesting refunds for Services) due to the termination of the Agreement and/or the DPA in the situation described in this paragraph (excluding the obligations relating to the termination of this DPA set forth below).

2.3.3 Orca will not be liable in the event of any claim brought by a third party, including, without limitation, a Data Subject, arising from any act or omission of Orca, to the extent that such is a result of Customer's instructions.

2.4 **California Consumer Privacy Act**. To the extent that the CCPA applies to the Processing of Personal Data subject to this DPA and the Agreement, Orca (acting as a Service Provider) will not: (i) retain, use, or disclose any Customer's Personal Data, for any purpose other than as described in this DPA and in the Agreement; or (ii) sell Customer Personal Data to any third party. Notwithstanding anything to the contrary, Orca is hereby authorized to share Personal Data with the authorized Sub-processors. For purposes of applicable law, both parties agree that there is no sale of Personal Data involved in Orca's provision of the Services to Customer. For the avoidance of doubt, Customer does not provide Personal Data to Orca for any valuable consideration. For purposes of this Section, all terms used but not defined shall have the meaning ascribed to them in the CCPA.

2.5 **Details of the Processing.** The subject-matter of Processing of Personal Data by Orca is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, as well as the types of Personal Data Processed and categories of Data Subjects under this DPA are further specified in Annex 1.B (Details of the Processing and Transfers) to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1 **Data Subject Request.** Orca shall, to the extent legally permitted, promptly notify Customer if Orca receives a request from a Data Subject to exercise the Data Subject's rights under Data Protection Laws and Regulations ("**Data Subject Request**"). Taking into account the nature of the Processing, Orca shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Orca shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Orca is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Orca's provision of such assistance.

4. ORCA PERSONNEL

4.1 **Confidentiality.** Orca shall ensure that its personnel engaged in the Processing of Personal Data have committed themselves to confidentiality and non-disclosure.

4.2 Orca may disclose and Process the Personal Data (a) as permitted hereunder (b) to the extent required by a court of competent jurisdiction or other Supervisory Authority and/or otherwise as required by applicable laws or applicable Data Protection Laws and Regulations (in such a case, Orca shall inform the Customer of the legal requirement before the disclosure, unless that law prohibits such information on important grounds of public interest), or (c) on a "need-to-know" basis under an obligation of confidentiality to its legal counsel(s), data protection advisor(s) and accountant(s).

5. AUTHORIZATION REGARDING SUB-PROCESSORS

5.1 **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) Orca's Affiliates may be used as Sub-processors; and (b) Orca and/or Orca's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services.

5.2 **List of Current Sub-processors.** The list of Sub-processors used by Orca as of the last signature date of this DPA is attached hereto as Annex 3 ("**Sub-processor List**"). The Sub-processor List is hereby approved by Customer.

5.3 **Notification and Objection rights for New Sub-processors.** Orca shall notify Customer ten (10) days in advance prior to use of new Sub-processor. Customer may reasonably object to Orca's use of a new Sub-processor for reasons related to Data Protection Laws and Regulations by notifying Orca promptly in writing within three (3) business days after receipt of Orca's notice and such written objection shall include the reasons related to Data Protection Laws and Regulations for objecting to Orca's use of such

new Sub-processor. Failure to object to such new Sub-processor in writing within three (3) business days following Orca's notice shall be deemed as acceptance of the new Sub-Processor. In the event Customer reasonably objects to a new Sub-processor, as permitted in the preceding sentences, Orca will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If Orca is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those Services which cannot be provided by Orca without the use of the objected-to new Sub-processor by providing written notice to Orca provided that all amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Orca. Until a decision is made regarding the new Sub-processor, Orca may temporarily suspend the Processing of the affected Personal Data. Customer will have no further claims against Orca due to the termination of the Agreement and/or the DPA in the situation described in this paragraph.

5.4 **Agreements with Sub-processors**. Orca shall respect the conditions referred to in Articles 28.2 and 28.4 of the GDPR when engaging another processor for Processing Personal Data provided by Customer. This Section 5 shall not apply to subcontractors of Orca which provide ancillary services to support the performance of the DPA. This includes, without limitation, telecommunication services, maintenance and user service or auditors.

6. SECURITY

6.1 **Controls for the Protection of Personal Data**. Orca shall maintain all industry-standard technical and organizational measures required pursuant to Article 32 of the GDPR for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data, in accordance with the Security Documentation which are hereby approved by Customer. Orca regularly monitors compliance with these measures. Upon the Customer's request, Orca will assist Customer, at Customer's cost, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the processing and the information available to Orca.

6.2 **Third-Party Certifications and Audits.** Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement and this DPA, Orca shall make available to Customer that is not a competitor of Orca (or Customer's independent, third-party auditor that is not a competitor of Orca) a copy of Orca's then most recent third-party audits or certifications which are relevant and necessary in order to demonstrate compliance with Data Protection Laws and Regulations in relation to Orca's technical and organizational security measures used to protect Personal Data in relation to the Services provided, as applicable (provided, however, that such audits, certifications and the results therefrom, including the documents reflecting the outcome of the audit and/or the certifications, shall only be used by Customer to assess compliance with this DPA and/or with applicable Data Protection Laws and Regulations, and shall not be used for any other purpose or disclosed to any third party without Orca's prior written approval and, upon Orca's first request, Customer shall return all records or documentation in Customer's possession or control provided by Orca in the context of the audit and/or the certification). At Customer's cost and expense, Orca shall allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller (who is not a direct or indirect competitor of Orca) provided that the parties shall agree on the scope, timing and conditions of such audits and inspections.

7. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

Orca maintains security incident management policies and procedures and, to the extent required under applicable Data Protection Laws and Regulations, shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, including Personal Data, transmitted, stored or otherwise Processed by Orca or its Sub-processors of which Orca becomes aware (a "**Personal Data Incident**"). Orca shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as Orca deems necessary and reasonable in order to remediate the cause of such a Personal Data Incident to the extent the remediation is within Orca's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's users. In any event, Customer will be the party responsible for notifying Supervisory Authorities and/or concerned Data Subjects (where required by Data Protection Laws and Regulations).

8. RETURN AND DELETION OF PERSONAL DATA

Subject to the Agreement, Orca shall, at the choice of Customer, delete or return the Personal Data to Customer after the end of the provision of the Services relating to processing, and shall delete existing copies unless applicable law requires storage of the Personal Data. In any event, to the extent required or allowed by applicable law, Orca may retain one copy of the Personal Data for evidence purposes and/or for the establishment, exercise or defense of legal claims and/or to comply with applicable laws and regulations. If the Customer requests the Personal Data to be returned, the Personal Data shall be returned in the format generally available for Orca's Customers.

9. AUTHORIZED AFFILIATES

9.1 **Contractual Relationship.** The Parties acknowledge and agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Orca. Each Authorized Affiliate agrees to be bound by the obligations under this DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions therein by an Authorized Affiliate shall be deemed a violation by Customer.

9.2 **Communication.** The Customer shall remain responsible for coordinating all communication with Orca under the Agreement and this DPA and shall be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates. Orca's legal representative may be reached at: Privacy@orca.security.

10. TRANSFERS OF DATA

10.1 **Transfers to countries that offer adequate level of data protection**: Personal Data may be transferred from the EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland) and the United Kingdom (collectively, "**EEA**") to countries that offer adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the Union, the Member States or the European Commission ("**Adequacy Decisions**"), without any further safeguard being necessary.

10.2 **Transfers from the EEA to Other Countries**: If the Processing of Personal Data includes transfers from the EEA to countries which do not offer an adequate level of data protection or which have not been subject to an Adequacy Decision ("**Other Countries**"), Orca may transfer Personal Data to Other Countries for the purposes of this DPA subject to the Standard Contractual Clauses ("**SCCs**"), which are hereby incorporated by reference. For the purpose of the SCCs:

(a) Customer (acting on behalf of itself and its Authorized Affiliates) shall be the "data exporter" and Orca and/or its Affiliates (as applicable) shall be the "data importer"

(b) Module Two of the SCCs shall apply as set forth in Annex 1.B;

(c) Clause 7 of the SCCs shall apply;

(d) Clause 9 of the SCCs, Option 2 shall apply and the method for appointing and time period for prior notice of Sub-processor changes shall be as set forth in Section 5 (Authorization Regarding Sub-processors) of this DPA;

(e) Clause 11 of the SCCs, the optional language shall be deleted;

(f) Clause 17 of the SCCs, Option 1 shall apply and the SCCs shall be governed by the laws of Ireland.

(g) in Clause 18(b) of the SCCs, disputes shall be resolved before the courts of Ireland;

(h) Annex 1.A. 1.B, 1.C, 2 and 3 of the SCCs shall be populated with the relevant information attached hereto, respectively.

10.3 **Transfers from the UK to Other Countries**: If the Processing of Personal Data includes transfers from the United Kingdom to Other Countries, Orca may transfer Personal Data to Other Countries for the purposes of this DPA subject to the SCCs and the UK Addendum ("**UK SCCs**), (controller to processor) with the below modifications or any future United-Kingdom approved addendum to apply the UK SCCs on transfers of Personal Data from the UK to Other Countries:

(a) The contact details of the Parties under the UK SCCs shall be populated with the relevant information of the parties under this DPA. For the avoidance of doubt. Customer shall be considered the Data Exporter and Orca the Data Importer. The date of the UK SCCs shall be the date of the execution of this DPA.

(b) Clause 9 shall be interpreted as references to the courts of England and Wales. Clause 11(3) shall be interpreted as the laws of England and Wales. Additional commercial clauses shall not be included.

(c) Appendix 1 and 2 of the UK SCCs shall be populated with the relevant information attached hereto, respectively.

11. TERMINATION

This DPA shall automatically terminate upon the termination or expiration of the Agreement under which the Services are provided. Sections 2.2, 2.3.2, 2.3.3, 8 and 12 shall survive the termination or expiration of this DPA for any reason.

12. RELATIONSHIP WITH AGREEMENT

In the event of any conflict between the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement.

13. AMENDMENTS

This DPA may be amended at any time by a written instrument duly signed by each of the Parties.

14. SIGNATURE

The Parties represent and warrant that they each have the power to enter into, execute, perform and be bound by this DPA.

You, as the signing person on behalf of Customer, represent and warrant that you have, or you were granted, full authority to bind Customer and, as applicable, its Authorized Affiliates to this DPA. If you cannot, or do not have authority to, bind the Customer and/or its Authorized Affiliates, you shall not supply or provide Personal Data to Orca.

By signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required or permitted under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent that Orca processes Personal Data for which such Authorized Affiliates qualify as the/a "data controller".

List of Annexes

- **Annex 1.A – The Parties for purposes of the SCCs**
- **Annex 1.B- Description of Processing and Transfers**
- **Annex 1.C - Competent Supervisory Authority**
- **Annex 2- Security Measures Under the SCCs**
- **Annex 3- List of Sub-Processors**

ANNEX 1.A - THE PARTIES FOR PURPOSES OF THE SCCS

Data Exporter:	
Name:	The counterparty under the Agreement and its Affiliates
Address:	The counterparty's address under the Agreement
Contact person's name, position and contact details:	The contact under the Agreement
Activities relevant to data transferred under these Clauses:	Relevant activities are described in Annex 1.B below.
Effect**:**	Insofar as Data Protection Laws and Regulations require the execution of this Annex 1.A, the Parties' signatures or acceptance of the Agreement shall apply here as well.
Role (controller / processor):	Controller

Data Importer:	
Name:	Orca Security Inc.
Address:	1455 NW Irving St., Suite 390 Portland, OR 97209
Contact person's name, position and contact details:	Oded Edri, CFO and Acting COO, oded.edri@orca.security
Activities relevant to data transferred under these Clauses:	Relevant activities are described in Annex 1.B below.
Effect:	Insofar as Data Protection Laws and Regulations require the execution of this Annex 1.A, the Parties' signatures or acceptance of the Agreement shall apply here as well.
Role (controller / processor):	Processor

ANNEX 1.B - DETAILS OF THE PROCESSING AND TRANSFERS

	Description
Categories of data subjects:	Employees, Suppliers, Customers, Candidates, Contractors and others (all as applicable with respect to the Personal Data that resides on Data Controller's cloud environment)
Categories of personal data:	Names, Emails, Titles, Positions, and other data (all as applicable with respect to the Personal Data that resides on Data Controller's cloud environment)
Sensitive data:	Not Applicable
Subject matter / Nature of the processing:	The Orca Security Full Visibility Platform is used to provide Orca's customers with cloud security risk detection services. The Solution scans the cloud environment of the customer, according to the customer's pre-set preferences (i.e. the customer may decide which cloud environments will be scanned), in a Read-Only ("Side Scanning") format without any modification or long term storage of customer data on to Orca's systems (Orca does not store confidential information and/or raw personally identifiable information that resides on customer's cloud environment). The security metadata which contains pseudonymized Personal Data is masked at source. 1. Providing the Service(s) to Customer, including, providing support and technical maintenance, if agreed in the Agreement. 2. Scanning customer compute environment, including ones that include personal data, with the purpose to 1) detect security issues such as vulnerabilities, misconfiguration, compromises and other security issues and 2) provide the customer with detailed information about his environment. 3. Presenting customer with the outcome of scanning as written at section #2 above. 4. Setting up profile(s) for users authorized by Customer. 5. For Orca to comply with documented reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement.
Period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	The duration of Processing will be as designated in the Agreement.
SCCs Module (if applicable)	Module Two
Purpose(s) of the data transfer and further processing (if applicable):	To provide the Services to Customer as described in the Agreement.
Frequency of the transfer (if applicable):	Continuous with the use of the Services.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	As described in this DPA and Annex 3.

ANNEX 1.C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority is the Irish Supervisory Authority.

ANNEX 2- SECURITY MEASURES UNDER THE SCCS

ADDITIONAL TECHNICAL AND ORGANIZATIONAL MEASURES DESCRIPTION:

1. Physical Access Controls: Orca Security shall take reasonable measures, such as security personnel and secured buildings and factory premises, to (i) prevent unauthorized persons from gaining access to Personal Data (ii) manage, monitor and log movement of persons into and out of Orca Security facilities, and (iii) guard against environmental hazards such as heat, fire, and water damage.

2. System Access Controls: Orca Security shall take reasonable measures to prevent unauthorized use of Personal Data. These controls may include, among other controls, authentication via passwords and two-factor authentication, documented authorization processes, documented change management processes, logging of access on several levels, system audit or event logging, and related monitoring procedures to proactively record user access and system activity for routine review.

3. Data Access Controls: Orca Security shall take reasonable measures to ensure that Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted, and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access; and, that Personal Data cannot be read, copied, modified, or removed without authorization in the course of Processing.

4. Access Policy: In addition to the access control rules set forth in Sections 1–3 above, Orca Security shall implement an access policy under which access to its system environment, to Personal Data, and to other data is restricted to authorized personnel only.

5. Transmission Controls: Orca Security shall take reasonable measures to ensure it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged so Personal Data cannot be read, copied, modified, or removed without authorization during electronic transmission or transport.

6. Input Controls: Orca Security shall take reasonable measures to ensure that it is possible to check and establish whether and by whom Personal Data has been entered into data Processing systems, modified, or removed. Orca Security shall take reasonable measures to ensure that: (i) the Personal Data source is under the control of Customer; and (ii) Personal Data integrated into Orca Security's systems is managed by secured file transfer from Customer.

7. Data Backup: Orca Security shall ensure that backups are made on a regular basis, are secured, and are encrypted when storing Personal Data to protect against accidental destruction or loss when hosted by Orca Security.

8. Logical Separation: Orca Security shall ensure that Personal Data is logically segregated on Orca Security's systems to ensure that Personal Data that is collected for different purposes can be Processed separately.

9. Organizational Management: Orca Security shall maintain a dedicated staff responsible for the development, implementation, and maintenance of Orca Security's data privacy and information security programs.

10. Audit: Orca Security shall maintain audit and risk assessment procedures for the purposes of periodic review and assessment of risks to the organization, monitoring and maintaining compliance, and reporting the condition of its information security and compliance to senior internal management.

11. Policies: Orca Security shall maintain data protection and Information security policies and make sure that policies and measures are regularly reviewed and where necessary, improve them.

12. Operations: Orca Security shall maintain operational procedures and controls to provide for configuration, monitoring, and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Customer possession.

13. Incident Response: Orca Security shall maintain incident / problem management procedures designed to investigate, respond to, mitigate and notify of events related to Customer's data or information assets.

14. Network Security: Orca Security shall implement network security controls, such as enterprise firewalls, layered DMZ architectures, intrusion detection systems, and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

15. Risk Management: Orca Security shall utilize vulnerability assessment, patch management, and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

16. Business Continuity: Orca Security shall maintain business resiliency/continuity and disaster recovery procedures, as appropriate, designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

ANNEX 3

LIST OF SUB-PROCESSORS

Entity Name	Purpose of Processing	Applicability	Location
The engaging entity, defined under the Agreement as "Company", shall not be considered as a "Sub-processor"			
Orca Security Ltd.	Providing support services, maintenance and management of the services, technical services	All Orca Security Customers	Israel
Orca Security, Inc.	Providing support services, maintenance and management of the services, technical services	All Orca Security Customers	United States
Orca Security UK Ltd.	Providing support services, maintenance and management of the services, technical services	All Orca Security Customers	United Kingdom
Orca Security Australia Pty Ltd.	Providing support services, maintenance and management of the services, technical services	All Orca Security Customers	Australia

Entity Name	Purpose of Processing	Applicability	Location
Amazon Web Services	Hosting the Orca Security Platform	The region for hosting is determined by Customer's preference upon setup of an Account	Germany, Frankfurt (eu-central-1)
			U.S., N. Virginia (us-east-1)
			Australia, Sydney (ap-southeast-2)
			US, GovCloud West (us-gov-west-1)
			India, Mumbai (ap-south-1)
			Israel (il-central-1)
			Brazil (sa-est-1)
Entity Name	**Purpose of Processing**	**Applicability**	**Location**
Microsoft Azure (Optional)	Scanning Customer's Workloads	Relevant if Customer scans Workloads of this Sub-Processor	Dynamically runs in the same data center locations as the Customer's environment
Google Cloud Platform (Optional)			
Oracle (Optional)			
AWS GovCloud (Optional)			
Alibaba Cloud (Optional)			
AWS China (Optional)			
Azure China (Optional)			
VMWare (Optional)			

Note: The list above is not an exhaustive list of optional Sub-Processors, by connecting any additional cloud environment to Orca Security's Platform you agree that Orca Security may use such cloud environment provider as an additional Sub-Processor.

Entity Name	Purpose of Processing	Applicability	Hosting Country
Snowflake	Processing security scan metadata and deriving insights	'Off' by default unless Customer confirms within the Platform.	United States or EU database (per Customer's cloud location).
Intercom	Providing a support chatbot within the Platform	Applicable to all customers and may be "switched off" from within the Platform	United States
Salesforce	Storing support tickets	Applicable to all customers	Germany