odaseva

ODASEVA - MASTER SUBSCRIPTION AGREEMENT

THIS AGREEMENT GOVERNS YOUR SUBSCRIPTION TO AND USE OF THE SERVICES.

Table of Contents

1. DEFINITIONS AND INTERPRETATION

1.1. Definitions

"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.

"Agreement" means this Master Subscription Agreement.

"Beta Services" means Our services that are not generally available to customers.

"Documentation" means Our online user guides, documentation, and help and training materials, as updated from time to time, accessible via Our website or login to the applicable Service.

"Intellectual Property Rights" means patents, utility models, rights to inventions, copyright and neighbouring and related rights, moral rights, trade marks and service marks, business names and

domain names, rights in get-up and trade dress, goodwill and the right to sue for passing off or unfair competition, rights in designs, rights in computer software, database rights, rights to use, and protect the confidentiality of, confidential information (including know-how and trade secrets) and all other intellectual property rights, in each case whether registered or unregistered and including all applications and rights to apply for and be granted, renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world.

"**Losses**" has the meaning as set out in Section 8.1 (Indemnification by Us).

"Malicious Code" means code, files, scripts, agents or programs intended to do harm, including, for example, viruses, worms, time bombs and Trojan horses.

"Order Form" means an ordering document specifying the Services to be provided hereunder that is entered into between You and Us or any of Our Affiliates, including any addenda and supplements thereto. By entering into an Order Form hereunder, an Affiliate agrees to be bound by the terms of this Agreement as if it were an original party hereto. The Order Form may include or refer to a statement of work ("**SOW**") describing professional Services and deliverables to be provided hereunder.

"**Personal Data**" means any information relating to an identified or identifiable natural person.

"Portal" means Our web-based platform accessible to Users at the following URL: https://platform.odaseva.com/CBR, used by Us to provide Services to You.

"SaaS Services" means Our commercially available proprietary cloud-based software solutions ("SaaS Services") together with related modifications, enhancements, improvements, updates, documentation and other related material, both now-existing and as hereafter developed which may be ordered by You and made accessible to Users through Our Portal. SaaS Services purchased by You (as distinguished from SaaS Services you receive free of charge) include Our standard support services at no additional cost.

"Services" means the products and services that are ordered by You under an Order Form and made available by Us, (including SaaS Services) and the Documentation.

"User" means an individual who is authorised by You to use a Service, for whom You have ordered the Service, and to whom You (or We at Your request) have supplied a user identification and password. Users may include, for example, Your employees, consultants, contractors and agents.

"We," "Us" or "Our" means Odaseva UK Limited with offices at 100 New Bridge Street, London, EC4V 6JA England

"You" or "Your" means the Customer and its Affiliates.

"Your Data" means electronic data and information submitted by or for You to the SaaS Services or collected and processed by or for You using the SaaS Services.

1.2. Interpretation

In this Agreement, the following rules apply:

(a) a person includes a natural person, corporate or unincorporated body (whether or not having separate legal personality);

(b) a reference to a statute or statutory provision is a reference to such statute or statutory provision as amended or re-enacted. A reference to a statute or statutory provision includes any subordinate legislation made under that statute or statutory provision, as amended or re-enacted;

(c) any phrase introduced by the terms 'including', 'include', 'in particular' or any similar expression shall be construed as illustrative and shall not limit the sense of the words preceding those terms;

(d) a reference to writing or written includes emails; and

(e) the Exhibits form part of this Agreement and shall have effect as if set out in full in the body of this Agreement and any reference to the Agreement includes the Exhibits.

2. OUR RESPONSIBILITIES

2.1. Provision of Services. We will (a) make the Services available to You pursuant to this Agreement and the applicable Order Forms and SOWs, (b) include Our standard customer support with purchased SaaS Services, and (c) use commercially reasonable efforts to make the SaaS Services available 24 hours a day, 7 days per week except for: (i) downtime for maintenance and (ii) any unavailability caused by force majeure events or circumstances beyond Our reasonable control, including, for example, act of government, flood, fire, earthquake, civil unrest, act of terror, strike or other labor problem (other than one involving Our employees).

In this regard, You understand that the access to and performance of the SaaS Services depends in part on the services of third parties which are necessary for its operation, including -among others- the internet service provider You selected, Your instance of the Salesforce.com application and other applications You license or use, and the data storage services provided by the cloud infrastructure provider You selected and which is set forth on the Order Form, e.g., Amazon Web Services or Microsoft. You specifically assume the risks of any failure or limitations of service by these third parties.

2.1. Protection of Your Data.

We will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Your Data. Those safeguards will include, but will not be limited to, measures for preventing access, use, modification or disclosure of Your Data by Our personnel except (a) to provide the Services to You and prevent or address related service or technical problems, (b) as compelled by law in accordance with Section 6.3 (Compelled Disclosure) below, or (c) as You expressly permit in writing.

2.2. Protection of Personal Data.

We will process Personal Data in accordance with the Data Processing Addendum attached hereto as Exhibit A.

2.3. **Our Personnel.** We will be responsible for the performance of Our personnel (including Our employees and contractors) and their compliance with Our obligations under this Agreement, except as otherwise specified herein.

2.4. **Beta Services.** From time to time, We may invite You to try Beta Services at no charge. You may accept or decline any such trial in Your sole discretion. Beta Services will be clearly designated as beta, pilot, limited release, developer preview, non-production, evaluation or by a description of similar import. Beta Services are for evaluation purposes and not for production use, are not considered "Services" under this Agreement, are not supported, and may be subject to additional terms. Unless otherwise stated, any Beta Services trial period will expire upon the earlier of one year from the trial start date or the date that a version of the Beta Services becomes generally available. We may discontinue Beta Services at any time in Our sole discretion and may never make them generally available. Subject to Section 9.3, We will have no liability for any Losses arising out of or in connection with a Beta Service.

3. USE OF SERVICES

3.1. **Right of Use**. Subject to You purchasing the User subscriptions in accordance with Section 3.2 (Subscriptions) and Section 4.1 (Fees), the restrictions set out in this Section 3 and the other terms and conditions of this Agreement, We hereby grant to You a non-exclusive, non-transferable right, without the right to grant sub-licences, to permit the Users to use the Services and the Documentation during the subscription term solely for Your internal business operations.

3.2. **Subscriptions.** Unless otherwise provided in the applicable Order Form, including for professional Services and deliverables as may be stated in an applicable SOW: (a) Services are purchased as subscriptions, (b) subscriptions may be added during a subscription term at the same pricing as the underlying subscription pricing, prorated for the portion of that subscription term remaining at the time the subscriptions are added, and (c) any added subscriptions will terminate on the same date as the underlying subscriptions.

3.3. **Usage Limits.**

(a) SaaS Services are subject to usage limits, including, for example, the quantities specified in Order Forms. Unless otherwise specified, a quantity in an Order Form refers (a) to volumes of records and salesforce organizations, and the SaaS Service may not be accessed beyond the number of ordered volumes and salesforce organizations, (b) to Users, and the SaaS Service may not be accessed by more than that number of Users; a User's password may not be shared with any other individual, and a User identification may be reassigned to a new individual replacing one who no longer requires ongoing use of the SaaS Services.

(b) If You exceed a contractual usage limit, We will work with You to seek to reduce Your usage so that it conforms to that limit. If, notwithstanding Our efforts, You are unable or unwilling to abide by a contractual usage limit, You will execute an Order Form for additional quantities of the applicable

Services promptly upon Our request, and/or pay any invoice for excess usage in accordance with Section 4.2 (Invoicing and Payment).

3.4. **Your Responsibilities.** You will (a) be responsible for User's compliance with this Agreement, (b) be responsible for the accuracy, quality and legality of Your Data and the means by which You acquired Your Data, (c) use all reasonable endeavours to prevent unauthorised access to or use of Services and/or the Documentation, and (d) without affecting Your other obligations under this Agreement, comply with all applicable laws and regulations with respect to Your activities under this Agreement.

3.5. **Usage Restrictions.** You will not, except as may be allowed by any applicable law which is incapable of exclusion by agreement between the parties: (a) make any Service available to, or use any Service for the benefit of, anyone other than You or Users, (b) sell, resell, license, sublicense, distribute, rent or lease any Service, or include any Service in a service bureau or outsourcing offering, (c) use a Service to store or transmit infringing, libellous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights, (d) use a Service to store or transmit Malicious Code, (e) interfere with or disrupt the integrity or performance of any Service or third-party data contained therein, (f) attempt to gain unauthorised access to any Service or its related systems or networks, (g) permit direct or indirect access to or use of any Service in a way that circumvents a contractual usage limit, (h) copy a Service or any part, feature, function or user interface thereof, (i) frame or mirror any part of any Service, other than framing on Your own intranets or otherwise for Your own internal business purposes or as permitted in the Documentation, (j) access any Service in order to build a competitive product or service, or (k) reverse engineer any Service.

4. FEES AND PAYMENT FOR SERVICES

4.1. Fees.

(a) In exchange for the SaaS Services, You will pay all fees specified in Order Forms. Except as otherwise specified herein or in an Order Form, (i) fees are based on SaaS Services purchased and not actual usage, provided that if actual usage exceeds the amount purchased, You shall pay for the excess used (ii) except as provided herein or therein, payment obligations are non-cancelable and fees paid are non-refundable, and (iii) quantities purchased cannot be decreased during the then current subscription term. Except with respect to excess usage, the fees for the SaaS Services are fixed during the initial term of the Order Form

(b) Notwithstanding the foregoing, You will pay for the professional Services and deliverables performed by Us pursuant to a SOW at the fixed fee or at the time-and-materials rate specified in the applicable SOW, or if no fixed fee or time-and-materials rate is specified in the SOW, at Our standard rates in effect at the time the SOW is executed. Any amount stated in a time-and-materials SOW is solely a good-faith estimate for budgeting by You and resource-scheduling purposes by Us and is not a guarantee that the professional Services will be completed for that amount; the actual amount may be higher or lower. If the estimated amount is expended, We will continue to provide the professional

Services under the same rates and terms. We will periodically update You on the status of the professional Services and the fees accrued under the SOW.

4.2. **Invoicing and Payment.** In order to purchase Services, You will provide Us with a valid purchase order or alternative document reasonably acceptable to Us. We will invoice You in advance and otherwise in accordance with the relevant Order Form. Unless otherwise stated in the Order Form, invoiced charges are due 30 days from the invoice date. You are responsible for providing complete and accurate billing and contact information to Us and notifying Us of any changes to such information.

4.3. **Overdue Charges.** If any invoiced amount is not received by Us by the due date, then without limiting Our rights or remedies, those charges may accrue late interest at the rate of 3% of the outstanding balance per annum, calculated on a daily basis.

4.4. **Suspension of Service and Acceleration.** If any amount owing by You under this Agreement for the Services is 30 or more days overdue, We may, without limiting Our other rights and remedies, accelerate Your unpaid fee obligations under this Agreement so that all such obligations become immediately due and payable, and suspend the Service to You until such amounts are paid in full. We will give You at least 10 days' prior notice that Your account is overdue, in accordance with Section 11.1 (Manner of Giving Notice), before suspending Services to You.

4.5. **Payment Disputes.** We will not exercise Our rights under Section 4.3 (Overdue Charges) or 4.4 (Suspension of Service and Acceleration) above if You are disputing the applicable charges reasonably and in good faith and are cooperating diligently to resolve the dispute.

4.6. **Taxes.** All amounts and fees stated or referred to in this agreement are exclusive of value added tax, which shall be added to Our invoice(s) at the appropriate rate.

4.7. **Future Functionality.** You agree that Your purchases are not contingent on the delivery of any future functionality or features, or dependent on any oral or written public comments made by Us regarding future functionality or features.

5. PROPRIETARY RIGHTS AND LICENSES

5.1. **Ownership.** Nothing in this Agreement shall constitute a transfer of any proprietary right by Us to You. The Service is protected by patent, copyright and other intellectual property laws. We, Our licensors and suppliers, own and retain all right, title and interest in and to the Intellectual Property Rights in the Service and Documentation, and any enhancements, modifications or derivative works thereof (including those suggested by You).

5.2. **Reservation of Rights.** We grant You a personal, non-exclusive and limited license to use the SaaS Service for the duration and pursuant to the terms and conditions specified in the Order Forms (the "**Subscription Term**"). All rights not specifically granted

to You in this Agreement are retained by Us. You acknowledge Our, and Our licensors', proprietary rights in the Service. We retain all right, title and interest in and to the Service. You acknowledge and agree that (i) no configuration or deployment of the Service shall affect or diminish Our rights, title, and interest in and to the Service; and (ii) if You suggest any new features, functionality or performance for the Service that is subsequently incorporated into the Service, We own and retain all right, title and interest in and to the Intellectual Property Rights in such suggestions. You acknowledge that the Service incorporating such new features, functionality, or performance shall be Our sole and exclusive property and all such suggestions shall be free from any confidentiality restrictions that might otherwise be imposed upon Us.

5.3. **Your Data.** Subject to the limited rights granted by You hereunder, We acquire no right, title or interest from You or Your licensors under this Agreement in or to Your Data, including any Intellectual Property Rights therein.

6. CONFIDENTIALITY

6.1. **Definition of Confidential Information.** "Confidential Information" means all information disclosed by a party ("Disclosing Party") to the other party ("Receiving Party"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Your Confidential Information includes Your Data; Our Confidential Information includes the Services; and Confidential Information of each party includes the terms and conditions of this Agreement and all Order Forms (including pricing), as well as business and marketing plans, technology and technical information, product plans and designs, and business processes disclosed by such party. However, Confidential Information does not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party.

6.2. **Protection of Confidential Information.** The Receiving Party will use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but not less than reasonable care). The Receiving Party shall: (i) not to use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement, and (ii) except as otherwise authorised by the Disclosing Party in writing, limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees and contractors who need that access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party containing protections not materially less protective of the Confidential Information than those herein. Neither party will disclose the terms of this Agreement or any Order Form to any third party other than its Affiliates, legal counsel and accountants without the other party's prior written consent, provided that a party that makes any such disclosure to its

Affiliate, legal counsel or accountants will remain responsible for such Affiliate's, legal counsel's or accountant's compliance with this Section 6.2.

6.3. **Compelled Disclosure.** The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior notice of the compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure.

7. REPRESENTATIONS, WARRANTIES, EXCLUSIVE REMEDIES AND DISCLAIMERS

7.1. **Representations.** Each party represents that it has validly entered into this Agreement and has the legal power to do so.

7.2. **Our Warranties.** We warrant that (a) the Services shall perform substantially in accordance with the Documentation at all times during the term of this Agreement, and (b) We will not introduce Malicious Code into Your systems. For any breach of a warranty in this Section 7.2, Your exclusive remedy shall be as provided in Section 10.3 (Termination) and Section 10.4 (Refund or Payment upon Termination) below.

7.3. **Disclaimers.** Except as expressly provided in this Agreement: (i) the Services and Documentation are provided to You on an "as is" basis, and (ii) all warranties, representations, conditions and all other terms of any kind whatsoever implied by statute or common law are, to the fullest extent permitted by applicable law, excluded from this Agreement. We do not warrant that use of the Service will be uninterrupted or error-free, and You acknowledge that the Service web site may, from time to time, be temporarily shut down due to routine maintenance or resolution of errors. Beta Services are provided "as is," exclusive of any warranty whatsoever. Each party disclaims all liability and indemnification obligations for any harm or damages caused by any third party hosting providers.

8. MUTUAL INDEMNIFICATION

8.1. **Indemnification by Us.** We will indemnify, defend and hold harmless You and Your Affiliates, officers, directors, and employees against any and all third party claims, demands, suits, actions, and proceedings (each a "**Claim**" and collectively, the "Claims") and all related liabilities, losses, expenses, damages and costs including reasonable legal fees and expenses (collectively, the "Losses") made or brought against You by a third party alleging that the Service or portions of components thereof, or the use thereof in accordance with this Agreement, infringes, causes the infringement or misappropriates any Intellectual Property Right of any third party ("Claim Against You"), provided that You (a) promptly give Us written notice of the Claim Against You, (b) give Us sole control of the defence and settlement of the Claim Against You (except that We may not settle any Claim Against You without Your prior written consent, which shall not be unreasonably withheld), and (c) give Us all reasonable assistance in the defence and settlement of such Claim, at Our expense. If

We receive information about an infringement or misappropriation Claim related to a Service, We may in Our discretion and at no cost to You (i) modify the Service so that it is no longer infringing or misappropriating, (ii) obtain a license for Your continued use of that Service in accordance with this Agreement, or (iii) terminate Your subscriptions for that Service upon 30 days' written notice and refund You any prepaid fees covering the remainder of the term of the terminated subscriptions. The above defence and indemnification obligations do not apply to the extent a Claim Against You arises from Your breach of this Agreement or the combination of the Services by You with any of Your own Intellectual Property Rights or the Intellectual Property Rights of a third party.

8.2. **Indemnification by You.** You will indemnify, defend and hold harmless Us and Our Affiliates, officers, directors, and employees (each an "Odaseva Indemnified Party") against any and all Claims and all related Losses made or brought against an Odaseva Indemnified Party by a third party alleging that Your Data, or Your use of any Service in breach of this Agreement, infringes or misappropriates such third party's Intellectual Property Rights or violates applicable law (a "Claim Against Us"). We will promptly give You written notice of the Claim Against Us, (b) give You sole control of the defence and settlement of the Claim Against Us (except that You may not settle any Claim Against Us without Our prior written consent, which shall not be unreasonably withheld.), and (c) give You all reasonable assistance in the defence and settlement of such Claim, at Your expense.

8.3. **Exclusive Remedy.** This Section 8 states the indemnifying party's sole liability to, and the indemnified party's exclusive remedy against, the other party for any type of Claim described in this Section 8.

9. LIMITATION OF LIABILITY

9.1. **Limitation of Liability.** Subject to Section 9.3 (Liability that is Not Excluded), the aggregate liability of each party together with all of its Affiliates in contract, tort (including negligence or breach of statutory duty), misrepresentation, restitution or otherwise, arising out of or related to this Agreement shall be limited to the total amount paid or payable by You and Your Affiliates hereunder for the Services giving rise to the liability in the twelve months preceding the first incident out of which the liability arose. The foregoing limitation will not limit Your and Your Affiliates' payment obligations under Section 4 (Fees and Payment for Services) above.

9.2. **Exclusion of Consequential and Related Damages.** Subject to Section 9.3 (Liability that is Not Excluded), in no event will either party or its Affiliates be liable whether based on a claim in contract, tort (including negligence or breach of statutory duty) or otherwise arising out of, or in relation to, this Agreement any (i) loss of profit, (ii) loss of revenue, (iii) loss of goodwill, or (iv) any indirect or consequential loss, however arising. .

9.3. **Liability that is Not Excluded**. Nothing in this Agreement shall limit or exclude either party's liability for: (i) death or personal injury caused by its negligence, or by the negligence of its personnel, agents or subcontractors; (ii) fraud or fraudulent

misrepresentation; (iii) breach of the terms implied by section 2 of the Supply of Goods and Services Act 1982 and section 12 of the Sale of Goods Act 1979; and (iv) any other liability which cannot be limited or excluded by applicable law.

10. TERM AND TERMINATION

10.1. **Term of Agreement.** This Agreement commences on the date executed by the parties and continues until all Order Forms have expired or have been terminated.

10.2. **Term of Purchased Subscriptions.** The term of each subscription shall be as specified in the applicable Order Form. Except as otherwise specified in an Order Form, subscriptions will automatically renew for additional periods equal to the expiring subscription term or one year (whichever is shorter), unless either party gives the other notice of non-renewal at least 60 days before the end of the relevant subscription term. The per-unit pricing during any renewal term will increase by up to 7% above the applicable pricing in the prior term, unless We provide You notice of different pricing at least 60 days prior to the applicable renewal term. Except as expressly provided in the applicable Order Form, renewal of promotional or one-time priced subscriptions will be at Our applicable list price in effect at the time of the applicable renewal. Notwithstanding anything to the contrary, any renewal in which subscription volume for any Services has decreased from the prior term will result in re-pricing at renewal without regard to the prior term's per-unit pricing.

10.3. **Termination.** A party may terminate this Agreement for cause (i) upon 30 days written notice to the other party of a material breach if such breach remains uncured at the expiration of such period, or (ii) immediately if the other party takes any step or action in connection with its entering administration, provisional liquidation or any composition or arrangement with its creditors (other than in relation to a solvent restructuring), applying to court for or obtaining a moratorium under Part A1 of the Insolvency Act 1986, being wound up (whether voluntarily or by order of the court, unless for the purpose of a solvent restructuring), having a receiver appointed to any of its assets or ceasing to carry on business or, if the step or action is taken in another jurisdiction, in connection with any analogous procedure in the relevant jurisdiction.

10.4. **Refund or Payment upon Termination.** If this Agreement is terminated by You in accordance with Section 10.3 (Termination), We will refund You any prepaid fees covering the remainder of the term of all Order Forms after the effective date of termination. If this Agreement is terminated by Us in accordance with Section 10.3 (Termination), You will pay any unpaid fees covering the remainder of the term of all Order Forms. In no event will termination relieve You of Your obligation to pay any fees payable to Us for the period prior to the effective date of termination.

10.5. **Your Data Portability and Deletion.** Upon request by You made within 15 days before the scheduled date of termination or expiration of this Agreement, We will make Your Data available to You for download directly on Our Portal before contract termination at no cost to You. Additionally, if You make the same request to Us within 15 days after the

effective date of termination or expiration of this Agreement, We will reactivate the Portal for a period of 10 days to allow You to download Your Data at no cost to You. Notwithstanding the above, after 15 days following the termination of this Agreement, We will have no obligation to maintain or provide Your Data, and will thereafter delete or destroy all copies of Your Data in Our systems or otherwise in Our possession, unless legally prohibited.

10.6. **Surviving Provisions.** The Sections titled "Fees and Payment for Services," "Proprietary Rights and Licenses," "Confidentiality," "Disclaimers," "Mutual Indemnification," "Limitation of Liability," "Refund or Payment upon Termination," "Your Data Portability and Deletion," "Notices, Governing Law and Jurisdiction," and "General Provisions" will survive any termination or expiration of this Agreement.

11. NOTICES, GOVERNING LAW AND JURISDICTION

11.1. **Manner of Giving Notice.** Except as otherwise specified in this Agreement, all notices, permissions and approvals hereunder shall be in writing and delivered by personal delivery or sent by email. A notice shall be deemed to have been given upon: (i) personal delivery, or (ii) the second business day after sending by confirmed email. You shall send any notices to Us at such address or email address as may have been notified to You by Us for such purposes. Billing-related notices to You shall be addressed to the relevant billing contact designated by You. All other notices to You shall be addressed to the relevant Services system administrator designated by You. The provisions of this Section 11.1 shall not apply to the service of any proceedings or other documents in any legal action.

11.2. **Governing Law and Jurisdiction.**

(a) The construction, validity and performance of this Agreement and all non-contractual obligations arising from or connected with this Agreement shall be governed by the laws of England.

(b) Each party irrevocably agrees to submit to the exclusive jurisdiction of the courts of England over any claim or matter arising under or in connection with this Agreement.

12. GENERAL PROVISIONS

12.1. **Force Majeure**. We shall have no liability to You under this Agreement if We are prevented from or delayed in performing Our obligations under this Agreement, or from carrying on Our business, or for any interruption of the Services, by acts, events, omissions or accidents beyond Our reasonable control, including, strikes, lock-outs or other industrial disputes (whether involving Our workforce or any other party), failure of a utility service or transport or telecommunications network, act of God, war, riot, pandemic or epidemic, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, accident, breakdown of plant or machinery, fire, flood, storm or default of suppliers or sub-contractors, provided that You are notified of such an event and its expected duration.

12.2. **Export Compliance.** The Services, other technology We make available, and derivatives thereof may be subject to export laws and regulations of the United States and other jurisdictions. Each party represents that it is not named on any U.S. government denied-party list. You shall not permit Users to access or use any Service in a U.S.-embargoed country (currently Cuba, Iran, North Korea, Sudan or Syria) or in violation of any U.S. export law or regulation.

12.3. **Anti-Corruption.** Each party agrees and undertakes to the other that in connection with this Agreement and the provision of Services contemplated by this Agreement, they will each respectively comply with anti-bribery and anti-corruption laws including the Bribery Act 2010. You have not received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from any of Our employees or agents in connection with this Agreement. Reasonable gifts and entertainment provided in the ordinary course of business do not violate the above restriction. If You learn of any violation of the above restriction, You will use reasonable efforts to promptly notify Our Legal Department.

12.4. **Entire Agreement and Order of Precedence.** This Agreement is the entire agreement between You and Us regarding Your use of Services and supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. No representation, undertaking or promise shall be taken to have been given or be implied from anything said or written in negotiations between the parties prior to this Agreement except as expressly stated in this Agreement. Neither party shall have any remedy in respect of any untrue statement made by the other upon which that party relied in entering into this Agreement (unless such untrue statement was made fraudulently). Without prejudice to the foregoing, the only remedy available to a party in respect of a breach of any representation which is incorporated into this Agreement shall be for breach of contract. No modification, amendment, or waiver of any provision of this Agreement will be effective unless in writing and signed by both parties. The parties agree that any term or condition stated in Your purchase order or in any other of Your order documentation (excluding Order Forms) shall not be binding on Us. In the event of any conflict or inconsistency among the following documents, the order of precedence shall be: (1) the applicable Order Form, (2) this Agreement, and (3) the Documentation.

12.5. **Assignment.** Neither party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the other party's prior written consent (not to be unreasonably withheld); provided, however, either party may assign this Agreement in its entirety (including all Order Forms), without the other party's consent to its Affiliate or in connection with a merger, acquisition, corporate reorganisation, or sale of all or substantially all of its assets. Notwithstanding the foregoing, if a party is acquired by, sells substantially all of its assets to, or undergoes a change of control in favour of, a direct competitor of the other party, then such other party may terminate this Agreement upon written notice. In the event of such a termination, We will refund to You any prepaid fees covering the remainder of the term of all subscriptions. Subject to the foregoing, this Agreement will bind and inure to the benefit of the parties, their respective successors and permitted assigns.

12.6. **Relationship of the Parties.** This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties. A party has no authority to bind, to contract in the name of or to create a liability for the other party in any way or for any purpose and neither party shall hold itself out as having authority to do the same.

12.7. **Waiver.** No failure or delay by either party in exercising any right under this Agreement will constitute a waiver of that right.

12.8. **Severability.** If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, and the remaining provisions of this Agreement will remain in effect.

12.9. **Third Party Rights.** Unless it expressly states otherwise, this Agreement does not confer any rights on any person or party (other than the parties to this Agreement and, where applicable, their successors and permitted assigns) pursuant to the Contracts (Rights of Third Parties) Act 1999.

12.10. **Counterparts.** This Agreement may be executed in counterparts, each of which shall be an original but all of which shall constitute one instrument.

EXHIBIT A
DATA PROCESSING ADDENDUM
(REVISED July 2023)

This Data Processing Addendum ("**DPA**") forms part of the Master Subscription Agreement ("**MSA**") or other written or electronic contract with Odaseva (such as an Order Form, an Evaluation Agreement, End-User License Agreement or any valid amendment thereto) regarding access and use of Odaseva's SaaS Services (including associated Odaseva offline or mobile components) (the "**Agreement**") and reflects the mutual agreement of the parties to the Agreement ("**Contracting Parties**") regarding the Processing of Personal Data submitted to the SaaS Services in accordance with the terms of the Agreement. Capitalized terms not otherwise defined in this DPA will have the respective meanings assigned to them in the applicable Agreement. In case of any conflict or inconsistency with the terms of the Agreement and except when expressly stipulated otherwise, this DPA will take precedence over the terms of the Agreement to the extent of such conflict or inconsistency.

If this DPA is signed on behalf of Odaseva, it shall become effective between Odaseva and the Counterparty to this DPA (the "**Parties**") on the date of its countersignature by the Counterparty. Otherwise, this DPA becomes effective upon its incorporation into the Agreement by mutual agreement of the Contracting Parties and as expressly evidenced in the Agreement. Odaseva may update the provisions of this DPA from time to time. The "Revised" date at the top of this DPA identifies the most recent update which supersedes and replaces the prior version between the Contracting Parties, provided that Odaseva has provided the Counterparty to this DPA with written notice of the update and Odaseva has not received a written objection to such update within ten (10) business days. Once effective, the term of this DPA shall be coterminous with the Agreement.

1. PARTIES TO THIS DPA

This DPA becomes effective between the Contracting Parties on the date first incorporated into the Agreement by reference ("**DPA Effective Date**"). The parties to this DPA shall be the same as the Contracting Parties to the Agreement.

If the countersigned entity to this DPA ("**Counterparty**") is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the Odaseva entity that is party to the Agreement is party to this DPA.

If the Counterparty to this DPA has executed an Order Form with Odaseva or its Affiliate pursuant to a MSA, but is not itself a party to the MSA, this DPA is an addendum to that Order Form (and renewals thereof) and the Odaseva entity that is party to such Order Form is party to this DPA, for the purposes of this DPA.

If the Counterparty to this DPA is not a party to an Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Counterparty who is a party to the Agreement executes this DPA.

If the Counterparty to this DPA is not a party to an Agreement directly with Odaseva, but indirectly via an authorized reseller of Odaseva's SaaS Services, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether any amendment to its agreement with that reseller may be required.

2. SCOPE OF THIS DPA

Odaseva has agreed to enter into this DPA with the Counterparty based on the Counterparty's belief that the data provided to the SaaS Services by the Counterparty and/or its Authorized Users ("**Principal Data**") may include Personal Data or Personal Information.

If and to the extent Odaseva processes Principal Data containing Personal Data from a Counterparty's Affiliate entity, the Counterparty is entering into this DPA on behalf of itself and its Affiliates to the extent required under applicable Data Protection Laws and Regulations. For purposes of this DPA only, and except where indicated otherwise, the term "Counterparty" shall include any relevant Affiliates of the Counterparty.

This DPA specifies the obligations and rights of the Contracting Parties under applicable Data Protection Laws and Regulations in connection with the Processing of Personal Data included in the Principal Data, lawfully collected and provided to the SaaS Services by the Counterparty and/or its Authorized Users. This DPA does not apply to the obligations of the Contracting Parties with respect to Personal Data not provided to the SaaS Services.

Upon entering into this DPA and where appropriate, the Contracting Parties shall be deemed to have signed and accepted the Standard Contractual Clauses incorporated herein by references.

3. ROLES AND RESPONSIBILITIES

Odaseva shall undertake as "**Processor**" a data Processing service on behalf of the Counterparty solely in connection with Odaseva's provision of SaaS Services to Counterparty under the terms of the Agreement. Odaseva shall process the Principal Data exclusively on behalf of and in accordance with the instructions of the Counterparty.

Within the scope of this DPA, the Counterparty shall as a "**Controller**" (or a "**business**" as defined under the CCPA) be solely responsible for compliance with the statutory provisions of the applicable Data Protection Laws and Regulations, in particular for the legality of the Personal Data provided to the SaaS Services as well as for the legality of the data Processing including any applicable requirement to provide notice to Data Subjects of the use of Odaseva as Processor (including where Counterparty is also a Processor, by ensuring that the ultimate Controller does so). For the avoidance of doubt, the Counterparty's instructions for the Processing of Personal Data shall comply with all applicable Data Protection Laws and Regulations. The Counterparty has sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Counterparty acquired Personal Data. The Counterparty specifically declares and guarantees that its use of the SaaS Services will not violate the rights of any Data Subject, including those who have opted-out of sales or other uses or disclosures of their Personal Data, to the extent applicable under Data Protection Laws and Regulations.

4. PROCESSING OF PERSONAL DATA

4.1 Odaseva's Processing of Personal Data. Odaseva shall only access and Process Personal Data on behalf of and in accordance with Counterparty's documented instructions for the following purposes: (i) Processing in accordance with the Agreement; (ii) Processing initiated by Counterparty or its Authorized Users in their use of the SaaS Services; and (iii) Processing to comply with other documented reasonable instructions provided by Counterparty (e.g., via email) where such instructions are consistent with the terms of the Agreement and with the Data Protection Laws and Regulations. Odaseva will alert the Counterparty if it reasonably believes that such instructions violate said Data Protection Laws and Regulations.

4.2 Details of the Processing. The subject-matter of Processing of Personal Data by Odaseva is the performance of the SaaS Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing,

the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 2 (Details of the Processing) to this DPA.

5. PERSONAL DATA INQUIRIES AND REQUESTS

Data Subject Request. Odaseva shall, to the extent legally permitted, promptly notify Counterparty if it receives a request from a Data Subject (or from a "**consumer**" as defined in the CCPA) to access, correct, restrict the use of, opt out of the sale or sharing of, or delete that person's Personal Data or if a Data Subject objects to the Processing thereof ("**Data Subject Request**"). Odaseva shall not respond to a Data Subject Request without Counterparty's prior written consent except to confirm that such request relates to Counterparty to which Counterparty hereby agrees. To the extent that Odaseva has the technical ability to address a Data Subject Request, and to the extent Odaseva is legally permitted to do so, and provided that such Data Subject Request is exercised in accordance with Data Protection Laws and Regulations, Odaseva shall upon Counterparty's request provide commercially reasonable assistance to facilitate addressing such Data Subject Request. To the extent legally permitted, Counterparty shall be responsible for any costs arising from Odaseva's provision of such assistance.

6. ODASEVA PERSONNEL

6.1 Confidentiality. Odaseva shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements.

6.2 Reliability. Odaseva shall take commercially reasonable steps to ensure the reliability of any Odaseva personnel engaged in the Processing of Personal Data.

6.3 Limitation of Access. Odaseva shall ensure that Odaseva's access to Personal Data is limited to those personnel performing the SaaS Services in accordance with the Agreement.

7. SUB-PROCESSORS

7.1 Appointment of Sub-processors. Counterparty acknowledges and agrees that (a) Odaseva's Affiliates may be retained as Sub-processors; and (b) Odaseva and Odaseva's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the SaaS Services. Odaseva or an Odaseva Affiliate has entered into a written agreement with each Sub-processor, including Amazon Web Services and salesforce.com, containing data protection obligations not less protective than those in this DPA with respect to the protection of Principal Data to the extent applicable to the nature of the SaaS Services provided by such Sub-processor.

7.2 Listing Sub-processors. The identity and country of location of Sub-processors are detailed in the then-current list Counterparty may request from Odaseva in writing. Odaseva may update its list of Sub-processors from time to time, provided that Odaseva has provided written notice of the update and has not received a written objection to such updates within ten (10) business days. In the event Counterparty objects to a new Sub-processor, Odaseva will use reasonable efforts to make available to Counterparty a change in the SaaS Services or recommend a commercially reasonable change to the Counterparty's configuration or use of the SaaS Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Counterparty. If Odaseva is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Counterparty may terminate the applicable Agreement with respect only to those SaaS Services which cannot be provided by Odaseva without the use of the objected-to new Sub-processor by providing written notice to Odaseva. Odaseva will refund Counterparty any prepaid fees covering

the remainder of the term of such Agreement following the effective date of termination with respect to such terminated SaaS Services, without imposing a penalty for such termination on Counterparty.

7.3 Liability. Odaseva shall be liable for the acts and omissions of its Sub-processors to the same extent Odaseva would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

8. SECURITY

Controls for the Protection of Principal Data. Odaseva shall maintain the appropriate technical and organizational measures described in Schedule 2 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.

9. AUTHORIZED AFFILIATES

9.1 Contractual Relationship. The Contracting Parties acknowledge and agree that, in the event the Counterparty 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 Odaseva and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 9 and Section 10. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the SaaS Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Counterparty.

9.2 Communication. The Counterparty which is identified as a signatory to the Agreement shall coordinate all communication with Odaseva under this DPA on behalf of itself and its Affiliates.

9.3 Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to the DPA with Odaseva, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

9.3.1 Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Odaseva directly by itself, the Contracting Parties agree that (i) solely the Counterparty that is a party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Counterparty that is a party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section 9.3.2, below).

9.3.2 The Contracting Parties agree that the Counterparty that is a party to the Agreement shall, when carrying out an on-site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Odaseva and its Sub-processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

10. LIMITATION OF LIABILITY

10.1 Each Contracting Party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Odaseva, whether in contract, tort or under any other theory

of liability, is subject to the 'Limitation of Liability' section of the Agreement which shall have precedence over any contradicting terms of this DPA and of the Standard Contractual Clauses, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

10.2 For the avoidance of doubt, Odaseva's and its Affiliates' total liability for all claims from the Counterparty and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Counterparty and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Counterparty and/or to any Authorized Affiliate that is a contractual party to any such DPA.

11. ADDITIONAL PROVISIONS FOR CALIFORNIA PERSONAL INFORMATION

11.1 Scope. This 'Additional Provisions for California Personal Information' section of the DPA will apply only with respect to Personal Information of California residents, as regulated by the CCPA.

11.2 Roles of the Contracting Parties. When Processing Personal Information hereunder, the Contracting Parties acknowledge and agree that Counterparty has the role of a Business and Odaseva has the role of a Service Provider, as defined in the CCPA.

11.3 Service Provider's Responsibilities. The Contracting Parties agree that Odaseva, in its role as a Service Provider, will process the Personal Information contained in Principal Data strictly for the purpose of performing the SaaS Services under the Agreement and this DPA (the "**Business Purpose**") or as otherwise permitted by the CCPA. Odaseva will comply with its applicable obligations under the CCPA and will provide the same level of protection as required under the CCPA. Odaseva agrees not to

(i) sell or share any Personal Information, as the terms "sell" and "share" are defined in the CCPA;

(ii) retain, use or disclose Personal Information outside of the express Business Purpose stated in the Agreement; or

(iii) combine the Counterparty's Personal Information processed by Odaseva with any other Personal Information Service Provider receives from, or on behalf of, another person or collects from its own, independent consumer interaction if and to the extent such combination would be inconsistent with limitations on Service Providers under the CCPA.

Odaseva will inform Counterparty, promptly without undue delay, if Odaseva cannot comply with its obligations as a Service Provider to Counterparty as required under the CCPA.

11.4 Counterparty's Responsibilities. Counterparties may: (1) take reasonable and appropriate steps agreed upon by the Contracting Parties to help ensure that Odaseva Processes Personal Information in a manner consistent with Counterparty's CCPA obligations; and (2) upon notice, take reasonable and appropriate steps agreed upon by the Contracting Parties to stop and remediate unauthorized Processing of Personal Information by Odaseva.

11.5 Additional Provisions of this DPA applicable to Personal Information. All provisions of this DPA which apply to Personal Data shall also apply to Personal Information. Notwithstanding the above, Sections 12.2, and 12.5 do not apply in connection with Personal Information processed under this DPA.

12. ADDITIONAL PROVISIONS FOR EEA PERSONAL DATA

12.1 **GDPR**. To the extent that the GDPR is applicable to any Personal Data within the Principal Data, Odaseva will Process Personal Data in accordance with the GDPR requirements directly applicable to Odaseva's provision of its SaaS Services.

12.2 **Assistance**. Upon the Counterparty's request, Odaseva shall provide Counterparty with reasonable cooperation and assistance needed to demonstrate the Contracting Parties' compliance with GDPR and/or to fulfil its obligation under the GDPR to carry out a data protection impact assessment related to the Counterparty or its Authorized Users' use of the SaaS Services, to the extent the Counterparty does not otherwise have access to the relevant information, and to the extent such information is available to Odaseva. Odaseva shall provide reasonable assistance to the Counterparty in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 12.2, to the extent required under the GDPR.

12.3 **Incidents.** Odaseva maintains the security incident management policies and procedures specified in Schedule 2 and shall notify the Counterparty without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Principal Data, including Personal Data, transmitted, stored or otherwise Processed by Odaseva or its Sub-processors of which Odaseva becomes aware (a "**Principal Data Incident**"). Odaseva shall make reasonable efforts to identify the cause of such Principal Data Incident and take those steps as Odaseva deems necessary and reasonable in order to remediate the cause of such a Principal Data Incident to the extent the remediation is within Odaseva's reasonable control. The obligations herein shall not apply to Principal Data Incidents or other data security incidents that are caused by the Counterparty or its Authorized Users.

12.4 **Transfer mechanisms for data transfers.** Subject to the additional terms in Schedule 1, the Standard Contractual Clauses will apply to any transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of all applicable European, Swiss and/or UK Data Protections Laws and Regulations, and orders of governmental authorities of the foregoing territories, to the extent such transfers are subject to such applicable Data Protections Laws and Regulations.

12.5 **Return and deletion of Principal Data.** Upon request by the Counterparty made before the scheduled date of termination or expiration of the Agreement, Odaseva will make the Principal Data available for download by the Counterparty directly on the Odaseva portal before contract termination at no cost to the Counterparty. Additionally, if the Counterparty makes the same request to Odaseva within thirty (30) days after the effective date of termination or expiration of this Agreement, Odaseva will reactivate the portal for a period of thirty (30) days to allow the Counterparty to download the Principal Data, all at no cost to the Counterparty. Notwithstanding the above, after thirty (30) days following the termination of the Agreement, Odaseva will have no obligation to maintain or provide the Principal Data, and will thereafter delete or destroy all copies of the Principal Data in its systems or otherwise in its possession, to the extent allowed by Data Protection Laws and Regulations.

13. GENERAL PROVISIONS

13.1 **Severability**. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

13.2 **Governing Law**. This DPA will be governed by and construed in accordance with the choice of law provision in the Agreement, unless otherwise required by Data Protection Laws and Regulations or the Standard Contractual Clauses.

14. DEFINITIONS

"**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.

"**Authorized Affiliate**" means any of Counterparty's Affiliate(s) which is permitted to use the SaaS Services pursuant to the Agreement between the Contracting Parties, but has not signed its own Agreement with Odaseva and is not a "Counterparty" as defined under the Agreement.

"**CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code 1798.100 et seq., and its implementing regulations, inclusive of the California Privacy Rights Act ("CCPA"), as may be amended from time to time.

"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

"**Counterparty**" means the business entity authorized to receive SaaS Services from Odaseva under the Agreement and which has entered into this DPA with the Odaseva entity in accordance with the provisions set forth herein.

"**Data Protection Laws and Regulations**" means all applicable laws and regulations applicable to the Processing of Personal Data under the Agreement.

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

"**EEA**" is the European Economic Area, an extension of the internal market of the European Union to three (3) countries beyond the European Union Member States, i.e.: Iceland, Lichtenstein and Norway.

"**GDPR**" means the 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).

"**Odaseva**" means the Odaseva entity which is a party to this DPA.

"**Odaseva Group**" means Odaseva and its Affiliates engaged in the Processing of Personal Data.

"**Personal Data**" means any information relating to an identified or identifiable natural person.

"**Personal information**" means, with respect to the CCPA, information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

"**Principal Data**" means the data provided to the SaaS Services by the Counterparty and/or its Authorized Users.

"**Process**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data, 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.

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller.

"**SaaS Services**" means the hosted services which the Counterparty may access and use under the terms of the Agreement and that are made available by Odaseva online via the applicable login page currently located at www.odaseva.com and other web pages designated by the Odaseva party to this DPA. The term SaaS Services excludes any other services which Odaseva may make commercially available (such as beta versions) to the Counterparty nor does it include consulting services, or customer support services.

"**Service Provider**" has the meaning set forth in Section 1798.140 of the CCPA.

"**Standard Contractual Clauses**" or "**SCCs**" means the "Controller to Processor" module of the Standard Contractual Clauses for the transfer of personal data to third countries, inclusive of any additional terms contained in Schedule 1 ("International Transfer Mechanisms") applicable to certain transfers, hereby incorporated into this DPA by reference and entered into by the Contracting Parties, upon the DPA Effective Date. Where the GDPR applies, the Standard Contractual Clauses are those clauses annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, available at: *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN* ("***EU-SCCs***"). Where the UK Data Protection Laws apply, the Standard Contractual Clauses shall be pursuant to UK Data Protection Laws as reflected in Schedule 1 of this DPA ("***UK-SCCs***"). Where the Swiss Data Protection Laws apply the Standard Contractual Clauses shall be pursuant to Swiss Data Protection Laws as reflected in Schedule 1 of this DPA ("**Swiss-SCCs**").

"**Sub-processor**" means any Processor engaged by Odaseva or a member of the Odaseva Group to Process Principal Data including Personal Data or Personal Information.

"**Swiss Data Protection Laws**" means all applicable data protection and privacy laws in force from time to time in Switzerland, including the Swiss Federal Data Protection Act 1992, as amended or replaced from time to time, such as by the Swiss Federal Data Protection Act 2020, when in force and applicable.

"**UK Data Protection Laws**" means any Data Protection Law in force in the United Kingdom from time to time, including the UK General Data Protection Regulation and the other applicable Data Protection Laws of the United Kingdom.

List of Schedules

Schedule 1: Transfer Mechanisms for European Data Transfers

Schedule 2: Details of the Processing

- Annex I: Data Processing Description
- Annex II: Technical and Organizational Security Measures

Schedule 3: List of Approved Sub-processors.

SCHEDULE 1 - TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS - ADDITIONAL TERMS FOR STANDARD CONTRACTUAL CLAUSES

1. Cross Border Data Transfer Mechanisms.

1.1. UK International Data Transfer Agreement ("IDTA") and UK International Data Transfer Addendum ("UK Addendum"). The parties agree that the IDTA and the UK Addendum will apply to Personal Data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for Personal Data. For data transfers from the United Kingdom that are subject to the IDTA and the UK Addendum, the IDTA and the UK Addendum will be deemed entered into (and incorporated into this Addendum by this reference). The competent supervisory authority in Annex I.C under Clause 13 shall be the UK Information Commissioner's Office.

1.2. 2021 Standard Contractual Clauses. The parties agree that the 2021 SCCs will apply to Personal Data that is transferred via the Services from the European Economic Area, Switzerland or Israel, either directly or via onward transfer, to any country or recipient outside the EEA or Switzerland that is not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for Personal Data. For data transfers from the EEA that are subject to the 2021 SCCs, the 2021 SCCs will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

a) Module Two (Controller to Processor) of the 2021 Standard Contractual Clauses will apply where Counterparty is a Controller of Personal Data and Odaseva is Processing such Personal Data.

b) Module Three (Processor to Processor) of the 2021 Standard Contractual Clauses will apply where Counterparty is a Processor of Personal Data and Odaseva is Processing such Personal Data.

c) For each Module, the following options apply:

(i) in Clause 7 of the 2021 SCCs, the optional docking clause will not apply;

(ii) in Clause 9(a) of the 2021 SCCs, Option 2 will apply and the time period for prior notice of Sub-processor changes will be as set forth in Section 8.2 of this Addendum;

(iii) in Clause 11 of the 2021 SCCs, the optional language will not apply;

(iv) in Clause 17 (Option 1), the 2021 SCCs will be governed by Irish law;

(v) in Clause 18(b) of the 2021 SCCs, disputes will be resolved before the courts of the Republic of Ireland.

1.3 FOR TRANSFERS SUBJECT TO THE PRIVACY LAWS OF SWITZERLAND

Transfers of Personal Data under this DPA which are subject to the Federal Data Protection Act of Switzerland ("FADP") to a data importer located outside Switzerland or the EEA and which is not covered by the list published by the Federal Data Protection and Information Commissioner of Switzerland (available hen each data exporter and data importer shall be in accordance with Module Two of the Standard Contractual Clauses as described in Section 1.2 of this Schedule 1 subject to the following ("Swiss SCCs"):

(i) if the Personal Data is subject to the FADP but not also covered by GDPR, then the following terms shall be deemed to amend the Standard Contractual Clauses:

- All references to the GDPR are to be understood as references to the FADP;
- The competent supervisory authority in Annex I.C under Clause 13 is the Federal Data Protection and Information Commissioner of Switzerland;
- Applicable law for contractual claims under Clause 17 is the law of Switzerland;
- The term "Member State" must not be interpreted in such a way as to exclude a data subject in Switzerland from the possibility of suing for his/her rights in Switzerland in accordance with Clause 18 c.; and
- Data of Swiss legal entities are subject to protection as personal data of data subjects under FADP.

(ii) if the Personal Data is subject to the FADP and GDPR, then the following terms shall be deemed to amend the Standard Contractual Clauses:

- The competent supervisory authority in Annex I.C under Clause 13 shall include the Federal Data Protection and Information Commissioner of Switzerland.

SCHEDULE 2 - DETAILS OF THE PROCESSING

(Including, Annexes I and II)

Annex I

Data Processing Description

This Annex I forms part of the DPA and describes the Processing that Odaseva (as the Processor or Sub-Processor, as applicable) will perform on behalf of the Counterparty (as the Controller).

A. LIST OF PARTIES

Controller(s) / Data exporter(s):

Counterparty Entity Name:	As set forth on the Order Form
Address:	As set forth on the Order Form
Contact person's name, position, and contact details:	As set forth on the Order Form
Activities relevant to the data processed/transferred:	Processing to carry out the SaaS Services pursuant to the Agreement entered into between Counterparty and Odaseva
Signature and date:	This Annex I shall automatically be deemed executed when the DPA becomes effective between the Contracting Parties
Role (controller/processor):	Controller

Processor(s) / Data importer(s):

Odaseva Entity Name:	As set forth on the Order Form
Address:	As set forth on the Order Form
Contact person's name, position, and contact details:	As set forth on the Order Form
Activities relevant to the data processed/transferred:	Processing to carry out the SaaS Services pursuant to the Agreement entered into between Counterparty and Odaseva
Signature and date:	This Annex I shall automatically be deemed executed when the DPA becomes effective between the Contracting Parties
Role (controller/processor):	Processor

B. DESCRIPTION OF PROCESSING / TRANSFER

Categories of Data Subjects:	Counterparty may submit Personal Data to the SaaS Services, the extent of which is determined and controlled by the Counterparty in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects: ● Prospects, customers, business partners and vendors of Counterparty (who are natural persons); ● Employees or contact persons of Counterparty's prospects, customers, business partners and vendors; ● Employees, agents, advisors, freelancers of Counterparty (who are natural persons); ● The Counterparty's Authorized Users of the SaaS Services
Purpose(s) of the data processing/transfer:	The objective of the processing of personal data to be carried out by Odaseva is the performance of the SaaS Services pursuant to the Agreement.
Categories of Personal Data:	Counterparty may submit Personal Data to the SaaS Services, the extent of which is determined and controlled by Counterparty in its sole discretion, and which may include, but is not limited to the following categories of Personal Data: o First and last name o Title o Position o Employer o Contact information (company, email, phone, physical business address) o ID data o Professional life data o Personal life data o Localization data
Sensitive data transferred (if applicable) and applied restrictions or safeguards:	Sensitive Data is out of scope
Frequency of the processing/transfer:	Continuous
Nature and subject matter of the processing:	Odaseva will Process Personal Data as necessary to provide the Counterparty with the following cloud-based data storage SaaS Services pursuant to the Agreement, in accordance with instructions provided by the Counterparty in its use of the SaaS Services: Salesforce data management services, including right-to-be forgotten, backups and restores services.
Duration of the processing	The duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms, plus the period from the expiry of the Agreement until deletion of the Personal Data by Odaseva in accordance with the terms of the Agreement.
Retention period (or, if not possible to determine, the criteria used to determine the period):	As above

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs):	Where the EU-SCCs apply, the French data protection authority in Paris. Where the UK SCCs apply, the UK Information Commissioner's Office. Where the Swiss SCCs apply, the Federal Data Protection and Information Commissioner

ANNEX II

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

1. INTRODUCTION

Security is at the core of Odaseva. To provide the highest degree of security and availability for the platform and SaaS services and to address the administrative, physical, and technical safeguards for the protection, security, confidentiality and integrity of personal data uploaded to the SaaS services, Odaseva maintains the policies, procedures and controls described in this Schedule. These measures are based on current best practices and industry standards, i.e., NIST 800-53, and cover areas including infrastructure monitoring and security operations, risk management, communication process and rigorous management of access rights to information within its information system. Odaseva reserves the right to update these controls from time to time provided that updates will not materially decrease the overall security of the SaaS services during a subscription term.

2. ENCRYPTION

As a no-view provider, Odaseva uses multiple layers of state-of-the-art encryption to protect customer data. Odaseva employees, administrators, and third party cloud providers do not have the ability to view customer data in clear text.

2.1. Customer data is granularly encrypted at the field and file level with the customer's provided AES-256 bit data encryption key.

2.2. Customers are given the choice between two key management solutions:

2.2.1. Bring Your Own Key - Odaseva stored
- Encryption key is managed by the customers through the Odaseva platform.
- Keys are stored encrypted and separate from systems storing processed data.
- Keys are retrievable in the event of loss through Odaseva emergency key loss process and break-glass procedure.

2.2.2. Bring Your Own Key Management System (KMS) Option
- Encryption key is managed by the customers on their own KMS.
- Customers have full control access to keys and may revoke access at any time.
- Key usage activities are logged on customer's KMS.
- Keys cannot be recovered by Odaseva in the event the key is lost.

2.3. Any integration or system access, in particular those concerning the Odaseva platform, will be implemented exclusively through state-of-the-art TLS protocols (TLS1.2 or greater).

3. ACCESS, IDENTIFICATION, AND AUTHENTICATION

Access to Odaseva's data and information systems is granted to individuals based on the principle of least privilege and need-to-know. Employees, contractors, or third parties are only granted access if it is required to perform job responsibilities.

3.1. Odaseva controls access to information, information assets and business processes based on business and security requirements.

3.2. Policies and procedures for account and access management have been established, documented, and reviewed based on business and security requirements.

3.3. Odaseva ensures authorized user accounts are registered, tracked, and periodically validated to prevent unauthorized access to information systems.

3.3.1. There is a formal documented and implemented user registration and deregistration procedure for granting and revoking access.

3.3.2. Privileged access includes any accounts or privileges that provide the user escalated access and rights to the information resource. The allocation and use of privileges to information systems and services are restricted and controlled.

3.3.3. Odaseva has set up a standard for the creation of strong passwords, the protection of those passwords, the prevention of their reuse, and the frequency of change. Passwords are controlled through a formal management process.

3.3.4. A formal record of all users registered and approved to use a system or service is maintained. All access rights are regularly reviewed by management via a formal documented process.

3.3.5. Odaseva has implemented segregation of duties for management of sensitive systems.

3.4. Odaseva prevents unauthorized access to operation systems.

3.4.1. All users have a unique identifier (user ID) for their personal use only, and authentication techniques are implemented to substantiate the claimed identity of a user. Generic accounts are not used.

3.4.2. Odaseva has implemented Role Based Access Control (RBAC) and access to systems is given on a need to know basis.

3.4.3. Systems for managing passwords are interactive and ensure quality passwords.

3.4.4. Multi-factor authentication is mandatory for all Odaseva employees and contractors accessing Odaseva information system.

3.4.5. Inactive sessions are shut down after a defined period of inactivity.

3.4.6. Maximum number of failed login attempts and lockout duration is enforced.

3.5. Odaseva ensures the security of information when using mobile computing devices and teleworking facilities.

3.5.1. Zero trust network access has been implemented for remote access to internal applications.

3.5.2. A formal policy is in place, and appropriate security measures (e.g., full-disk encryption, anti-malware, etc.) are adopted to protect against the risks of using mobile computing and communication devices.

3.5.3. End user devices are centrally managed and compliance enforcement is enabled for access to sensitive systems.

3.5.4. Policies, operational plans, and procedures are developed and implemented for teleworking activities.

3.6. Odaseva ensures access to the platform is granted to authorized customers only.

3.6.1. User accounts are linked to individual users of customers.

3.6.2. User account password follows strict requirements for length and complexity with period of validity and password history enforced.

3.6.3. Maximum number of failed login attempts and lockout duration is enforced.

3.6.4. Multi-factor authentication is available for accessing the Odaseva platform.

3.6.5. Customers can enable delegated single sign-on via their Salesforce instance.

3.6.6. Customer's administrators can manage the provisioning and deprovisioning of users and associated access as needed.

3.6.7. Role-based access controls are provided to customers to manage the permissions granted to their users.

4. Security Awareness and Training

4.1. All workforce members receive appropriate training concerning the Company's security policies and procedures. Such training is provided as part of employees onboarding and repeated annually.

4.2. Attendance and/or participation in such training is mandatory and is documented.

4.3. Latest versions of the security policies and measures are made available to all employees.

4.4. Specific training based on roles (secure coding, privileged users training, etc.) is delivered on an ongoing basis to respond to environmental and operational changes impacting the security of the organization.

4.5. Security reminders are sent to all employees. These reminders may address password security, malicious software, incident identification and response, access control, etc. These reminders can come through formal training, e-mail messages, discussions during staff meetings, or intranet articles.

4.6. Distribution of special notices providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures are communicated.
4.7. Phishing exercises are conducted on at least an annual basis.

5. Audits Logging and Monitoring

Odaseva analyzes and correlates audit records across different repositories using a security information and event management (SIEM) tool or log analytics tools for log aggregation and consolidation from multiple systems, applications, and devices.

Odaseva ensures information security events are monitored and recorded to detect unauthorized information processing activities in compliance with all relevant legal requirements.

5.1. Audit logs recording users and administrators activities, exceptions, and information security events are produced and kept for an agreed period to assist in future investigations and access control monitoring.
5.2. Procedures for monitoring use of information processing systems and facilities are established to check for use and effectiveness of implemented controls. The results of the monitoring activities shall be reviewed regularly.
5.3. Automated rules are in place to generate alerts for suspicious or abnormal behaviors. These alerts are regularly reviewed by Odaseva Security personnel.

6. Security Assessment and Vulnerability Management

Timely information about technical vulnerabilities of information systems being used is obtained, Odaseva's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

6.1. Odaseva hires independent third-party penetration testers to perform both network and web vulnerability assessments on the platform at least two times per year. For added security, penetration tests are performed by two separate vendors. The scope of these audits includes compliance against the Open Web Application Security Project (OWASP) Top 10 Web Vulnerabilities (www.owasp.org).
6.2. Odaseva performs periodic static code analysis assessments as part of its continuous monitoring program to help ensure application security controls are properly applied and operating effectively.
6.3. Vulnerabilities related to information and related assets are proactively identified through automated vulnerability scans and remediated according to the risk.
6.4. Vulnerabilities that pose a critical information risk are prioritized and patched early.

7. Configuration Management

7.1. Odaseva ensures that operating procedures are documented, maintained, and made available to all users who need them.
7.2. Systems are configured according to industry security baselines such as CIS Benchmarks.
7.3. Odaseva has established requirements governing the installation of software, enforces software installation restrictions and monitors compliance on a continual basis.
7.4. Critical systems are monitored with file integrity monitoring and intrusion detection technologies.
7.5. Changes to information assets and systems are controlled and archived.
7.6. Segregation of duties is enforced to reduce opportunities for unauthorized or unintentional modification or misuse of Odaseva's assets.

8. Business Continuity Management and Disaster Recovery

8.1. Odaseva ensures that strategies and plans are in place to counteract interruptions of business activities and to protect critical business processes from the effects of major failures of information systems or disasters, and to ensure their timely resumption.

8.1.1. Events that can cause interruptions to business processes are identified, along with the probability and impact of such interruptions and their consequences for information security.

8.1.2. Plans are developed and implemented to maintain or restore operations and to ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

8.1.3. A single framework of business continuity plans is maintained to ensure that all plans are consistent, to consistently address information security requirements and to identify priorities for testing and maintenance.

8.2. Industry leading cloud service providers, located globally, are used by Odaseva to deliver the SaaS service. As a result, Odaseva inherits the availability of 99.9% and the data durability of 99.999999999% from these cloud providers.

8.2.1. Customer data is processed and stored encrypted across multiple availability zones.

8.2.2. Versioning is used to preserve, retrieve, and restore previous versions of customer data backups, hence providing immutability.

8.2.3. Regular back-up copies of information and software are made and secured.

9. Information Security Incident Management

Odaseva has implemented an incident response plan to detect, respond to, and recover from security incidents. The company will regularly test the incident response plan to ensure it is effective. The goal of incident management is to reduce the risk inherent in securing information systems and information assets, and to mitigate any harmful events from the possible exploitation of vulnerabilities.

9.1. Odaseva ensures that information security events and weaknesses associated with information systems are handled in a manner allowing timely corrective action to be taken.

9.2. Information security events are reported to the Odaseva security team. All employees, contractors, and third-party users are made aware of their responsibility to report any information security events as quickly as possible.

9.3. Odaseva ensures a consistent and effective approach to the management of information security incidents.

10. Information Exchange and Protection

10.1. Odaseva protects the information it owns or possesses in its custody based on the nature of the information and the risk exposure to Odaseva, its workforce members, its customers, and its directors from inappropriate or undesired access, disclosure, or destruction. Odaseva prevents unauthorized disclosure, modification, removal or destruction of information assets, or interruptions of business activities.

10.2. Multiple safeguards are formally addressed prior to allowing the use of information systems for information exchange. Odaseva ensures the exchange of information within an organization and with any external entity is secured, protected, and carried out in compliance with relevant legislation and exchange agreements.

10.3. Formal policies, procedures, and controls are in place to protect the exchange of information using all types of communication mediums.

11. Physical and Environmental Protection

11.1. Odaseva policies require adequate physical safeguards to include both facility access controls, fire and natural disaster protection, and device and media controls to secure information systems and information assets.

11.2. Odaseva leverages trusted cloud providers to comply with these requirements and does not host any servers / network devices on Odaseva premises.

11.3. Physical protection and guidelines for working in areas are designed and applied.

12. Program Management and Security Policy

Odaseva has implemented and manages an ISMS aligned with ISO27001 guidelines.

12.1. The information security management system (ISMS) establishes the overall information security and protection program that is intended to complement the other security policies. The ISMS is formally documented, approved, actively monitored, reviewed, and updated to ensure that program security objectives are met. The ISMS sets up access controls that limit access to sensitive systems and information to the minimum necessary level to support organizational service delivery.

12.2. The information security policy and procedures are intended to ensure the confidentiality, integrity, and availability of information in any form created, received, maintained, or transmitted.

12.3. Management provides the direction for business objectives and relevant laws and regulations and demonstrates support for and commitment to information security through the issue and maintenance of information security policies across Odaseva.

13. Personnel Security

Odaseva ensures that employees, contractors, and third-party users are suitable for the roles for which they are being considered to reduce the risk of fraud, theft, or misuse of facilities.

13.1. Background verification checks on all candidates for employment and contractors are carried out in accordance with relevant laws, regulations, and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

13.2. Odaseva ensures agreements are signed by employees and contracted users of information assets on their security roles and responsibilities at the time of their employment or engagement, prior to sensitive access being granted.

13.3. Management requires employees, and where applicable, contractors and third-party users, to apply security in accordance with established policies and procedures of Odaseva.

13.3.1. All employees and contractors of Odaseva receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

13.3.2. There is a formal disciplinary process for employees who have violated security policies and procedures.

13.4. The access rights of all employees, contractors, and third-party users to information and information assets are removed upon termination of their employment, contract, or agreement, or adjusted upon a change of employment (i.e., upon transfer within Odaseva).

14. Personally Identifiable Information Processing and Transparency

14.1. A Data Protection Officer is appointed and is responsible for the development, implementation, and maintenance of policies, procedures, and processes regarding continuing compliance with privacy regulations such as GDPR, CCPA and the HIPAA Privacy Rule.

14.2. Odaseva ensures that PII is used solely for the purpose(s) specified in the privacy policy and only for a purpose that is compatible with the purpose for which the PII was collected.

14.3. The use and disclosure of PII for specific purposes are limited to explicit and legitimate purposes and must fulfill the stated purpose(s) or to abide by applicable laws.

14.4. Odaseva's privacy policy is published and available at: https://www.odaseva.com/assets/pdf/Odaseva-Privacy-Policy.pdf

15. Risk Management Program

A risk management strategy is developed and managed by management and documented in the risk management program. The risk management strategy defines Odaseva's risk tolerance, risk mitigation techniques, and risk assessment methodology.

15.1. Odaseva has developed and maintains a risk management program taking into account security needs and objectives, in order to identify risks and mitigate them in a timely manner.
15.2. Risks are continually evaluated and assessed, through threat monitoring and internal audits.

16. Asset Management

16.1. All assets, including information, are clearly identified and an inventory of all assets drawn up and maintained.
16.2. Rules for the acceptable use of information and assets associated with information processing systems are identified, documented, and implemented.
16.3. Information is classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.

17. Network Security

Network security is considered throughout the complete hardware and software lifecycle. Controls are implemented to ensure the security of information and the protection of connected services in terms of confidentiality, integrity, and availability. Appropriate logging and monitoring are applied to enable recording and detection of actions that may affect, or are relevant to, information security. Odaseva ensures the protection of information in networks and protection of the supporting network infrastructure.

17.1. Networks are managed and controlled to protect Odaseva from threats and to maintain security for the systems and applications using the network, including information in transit.
17.2. Odaseva prevents unauthorized access to networked services.
- 17.2.1. Appropriate authentication methods are used to control access by remote users including requirements of multifactor authentication
- 17.2.2. Groups of information services, users, and information systems are segregated on Odaseva's networks. Development environments are strictly separated from production instances.
- 17.2.3. Sensitive systems are dedicated and located in isolated computing environments.
- 17.2.4. Firewalling is in place to ensure that computer connections and information flows do not breach the access control policy of the business applications.

18. Secure Software Development and Information Security

Odaseva ensures the security of application system software and information throughout the development process, and project and support environments are strictly controlled.

18.1. Evolutions and enhancements of the Odaseva platform go through a threat modeling process to identify threats and specify security controls.
18.2. Secure development guidelines are maintained and distributed to the development team. Formal training on secure coding is in place.
18.3. The implementation of changes, including patches, service packs, and other updates and modifications, are controlled using a formal change control procedure, including following manual and automated code review and in-depth QA testing.
18.4. If any, outsourced software development is supervised and monitored by Odaseva.
18.5. Changes are communicated through release notes published on the Odaseva platform.

19. Third Party Risk Management

Odaseva ensures that third-party service providers maintain security requirements and levels of service as part of their service delivery agreements.

19.1. Odaseva has implemented a supplier management program. New third parties must go through a validation process covering contractual and security requirements.
19.2. Odaseva identifies and mandates information security controls to specifically address supplier access to Odaseva's information and information assets
19.3. Odaseva ensures that the security controls, service definitions, and delivery levels included in the third-party service delivery agreement are implemented, operated, and maintained by the third party.

20. COMPLIANCE AND INDEPENDENT EXTERNAL AUDITS

20.1. Odaseva ensures that all information systems adhere to all applicable laws, statutory, regulatory, or contractual clauses, and any business or security requirements.
20.2. Odaseva is currently ISO/IEC 27001:2013 certified
20.3. Odaseva undergoes an annual SOC2 Type II audit under SSAE-18 to independently verify the effectiveness of its information security practices, policies, procedures, and operations for the following Trust Services Criteria: Security, Availability, and Confidentiality.
20.4. Odaseva leverages leading global SaaS and cloud service providers for its web application, computing and storage for the Odaseva platform. AWS and Azure are top-tier facilities with several accreditations, including SOC1 - SSAE-18, SOC2, ISO 27001, and HIPAA.

odaseva

SCHEDULE 3 - Odaseva List of Sub-Processors

Odaseva uses the following affiliates and third-party suppliers to provide infrastructure, services and support to Odaseva in connection with provision of Services.

Name	Address	Country	GDPR data transfer mechanism	Purpose of processing
	Third Party Subcontractors/Sub-processors:			
Amazon Web Services	410 Terry Avenue North, Seattle, WA 98109 USA	US	SCCs	Cloud Hosting Services
Microsoft Corporation	One Microsoft Way Redmond, WA 98052, USA	US	SCCs	Azure cloud services for data hosting
Salesforce.com	415 Mission Street, San Francisco, California, 94105 U.S.A.	US	SCCs	CRM data hosting

Odaseva Affiliates as Subcontractors/Sub-processors:				
Odaseva Australia Pty Ltd [(c)]	Level 26 225 George Street Sydney NSW 2000 Australia	Australia	SCCs	Administrative shared services; customer support services; and/or professional services collaboration, as further specified below: shared administrative services and services ancillary to the Services provided by Supplier[1] with customer's prior consent enabling Supplier's performance of Tier 1 support services relating to the subscribed Services[2] internal collaboration and support for performance of professional services projects
Odaseva.com, Inc. [(a)] [(c)]	1411 Broadway, 16th Floor New York, NY 10018	United States	Data Privacy Framework	
Odaseva Technologies, SAS [(a)] [(c)]	144, Avenue Charles de Gaulle 92200 Neuilly-sur-Seine France	France	SCCs	
Odaseva Malaysia Sdn. Bhd. [(b)]	Level 6, Menara 1 Dutamas, Solaris Dutamas no.1, Jalan Dutamas 1, 50480 Kuala Lumpur	Malaysia	SCCs	
Odaseva Singapore Pte. Ltd. [(c)]	9 Straits View #06-07, Marina One West Tower, Singapore 018937	Singapore	SCCs	

[1] In accordance with Odaseva's role as a Controller and subject to Odaseva's privacy policy located at https://www.odaseva.com/

[2] temporary access by Odaseva's offshore staff to provide initial support assessments based on User's support ticket – and where access to data is limited to details on the support ticket; solely for the duration of ticket resolution; only for provision of Tier 1 support (entry level), and primarily for support during off-peak hours via-a-vis the Counterparty's time zone.

	Odaseva Affiliate Subcontractors/Sub-processors:			
Odaseva Technologies SAS	144, Avenue Charles de Gaulle, 92200 Neuilly-sur-Seine, France	France	SCCs	Administrative shared services; customer support; professional services collaboration
Odaseva Malaysia Sdn. Bhd.	Level 6, Menara 1 Dutamas, Solaris Dutamas no.1 Jalan Dutamas 1, 50480 Kuala Lumpur, Malaysia	Malaysia	SCCs	