

EXHIBIT A – DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**DPA**”) forms part of the Master Subscription Agreement or other written or electronic contract with Odaseva (such as an Order Form) 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 countersigned entity to this DPA (“**Counterparty**”) and Odaseva (the Counterparty and Odaseva being referred hereinafter together as the “**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 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.

1. SCOPE OF THIS DPA

Odaseva has agreed to enter into this DPA with the Counterparty based on the Counterparty’s desire to include Personal Data in the data submitted to the SaaS Services by the Counterparty and/or its Authorized Users (“**Principal Data**”) for processing by Odaseva.

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.

2. 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 written and documented instructions of the Counterparty.

Within the scope of this DPA, the Counterparty shall, as a “**Controller**”, warrant that Processing is in compliance with all 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 written and documented 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, to the extent applicable under Data Protection Laws and Regulations.

3. PROCESSING OF PERSONAL DATA

3.1 Odaseva's Processing of Personal Data. Odaseva shall only access and Process Personal Data on behalf of and in accordance with Counterparty's written and documented instructions for the following purposes: (a) Processing in accordance with the Agreement and Annex I of Schedule 1 attached hereto, including Processing initiated by Counterparty or its Authorized Users in their use of the SaaS Services; and (b) Processing to comply with other written, documented and 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 promptly alert the Counterparty if it reasonably believes that such instructions violate said Data Protection Laws and Regulations.

3.2 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 Annex I of Schedule 1 attached hereto.

4. PERSONAL DATA INQUIRIES AND REQUESTS

Odaseva shall, to the extent legally permitted, promptly notify Counterparty if it receives a request from a Data Subject exercising his or her rights, notably to access, correct, restrict the use of or delete that Data Subject's Personal Data or if a Data Subject objects to the Processing thereof and to data portability ("**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 reasonable assistance to facilitate addressing such Data Subject Request.

5. ODASEVA PERSONNEL

5.1 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 with confidentiality obligations not less protective than those set forth in the Agreement.

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

5.3 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.

6. SUB-PROCESSORS

6.1 Appointment of Sub-processors. Counterparty acknowledges and agrees that (a) Odaseva's Affiliates may be retained as Sub-processors; and (b) Odaseva may engage third-party Sub-processors in connection with the provision of the SaaS Services. Odaseva has entered into a written agreement with each Sub-processor, 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. Odaseva shall ensure that the Sub-processor complies with the obligations to which it is subject pursuant to this DPA and provide, at the Counterparty's request, a copy of such Sub-processor agreement and any subsequent amendments to Counterparty. To the extent necessary to protect business secrets or other confidential information, including Personal Data, Odaseva may redact the text of the Sub-processor agreement prior to sharing a copy.

6.2 Listing Sub-processors. The identity and country of location of Sub-processors are detailed here, in [Schedule 2](#) of this DPA. 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 of receipt of the notification.

Odaseva shall provide the Counterparty with the information necessary to enable Counterparty to exercise its right to object. 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 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.

6.3 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 and subject to the "Limitation of Liability" section of the Agreement.

7. SECURITY

Odaseva shall maintain the appropriate technical and organizational measures described in [Annex II of Schedule 1](#) 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. These measures will guarantee an appropriate level of security, taking into account the state of the art, the costs of implementation, in view of the risks entailed by Processing and the nature of the Personal Data to be protected.

8. LIMITATION OF LIABILITY

8.1 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 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.

8.2 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 the DPA shall apply in the aggregate for all claims under both the Agreement and this DPA, 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.

9. ADDITIONAL PROVISIONS

9.1 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.

9.2 Health Data. To the extent that the Principal Data submitted to the SaaS Services by Counterparty includes Personal Data on patients collected in France for the purposes of preventive treatment, diagnosis, healthcare or social care under Article [L. 1111-8](#) and Articles [R. 1111-9 and seq.](#) of the French Public Health Code (“**Health Data**”), the following will apply, in addition to the other provisions of this DPA:

(a) Counterparty agrees and understands that it is required to and shall comply with the enforceable reference systems of the Global Information Security Policy for the healthcare sector (“**PGSSI-S**”); and

(b) Odaseva and its concerned Sub-processors are both certified (“**HDS**”), as detailed in [Schedule 1](#), and will process such Health Data only on behalf and for the purposes of the SaaS Services in certified sites / *via* certified servers, all located in the EEA.

9.3 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, if and when appropriate, 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 9.3](#), to the extent required under the GDPR.

9.4 Disclosure requests. In the event Odaseva is requested or required under Data Protection Laws and Regulations to disclose Principal Data to public authorities, it undertakes to: (a) inform Counterparty of such request or requirement without undue delay (subject to compliance with Data Protection Laws and Regulations which may prevent it from informing Counterparty) in order to obtain Counterparty’s express and written consent to such disclosure; (b) with the assistance and at the costs of Counterparty, verify that law enforcement entities followed the laws and procedures in their jurisdictions before responding to a request; (c) with the assistance and at the costs of Counterparty, reject invalid legal requests (*e.g.*, requests that (i) exceed the authority or jurisdiction of the requesting entity, (ii) are not appropriately authorized, (iii) are not properly addressed, or (iv) are broad, unspecific or indiscriminate); (d) with the assistance and at the costs of Counterparty, challenge and or oppose (including by means of legal action), where possible, such request or requirement (including, notably, by advising that Odaseva does not own nor control the Principal Data it processes on behalf of Counterparty); or (e) allow, if possible, Counterparty (if it so decides) to participate in any action undertaken to oppose such disclosure. In support of the above, Odaseva may provide Counterparty’s basic contact information to the requesting entity in order to redirect its request.

9.5 Incidents. Odaseva maintains the security incident management policies and procedures specified in [Schedule 1](#) 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**”). Such notification shall contain, at least: (a) a description of the nature of the Principal Data Incident (including, where possible, the categories and approximate number of Data Subjects and data records concerned); (b) the details of a contact point where more information concerning the Principal Data Incident can be obtained; (c) its likely consequences and the measures taken or proposed to be taken to address the Principal Data Incident, including to mitigate its possible adverse effects. Where Odaseva cannot provide all this information at the same time, the information may be provided in phases without undue delay. 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.

9.6 Audit. Except in case of breach of this DPA, Principal Data Incident or Supervisory Authority request, the Counterparty shall be entitled to conduct once per contractual year Personal Data protection audit or to have such audit conducted by an independent and recognized expert chosen by the Counterparty, which is not a direct or indirect competitor of Odaseva and is bound by strict confidentiality obligations. Such audit shall be limited to the analysis of compliance of Odaseva with this DPA and the Data Protection Laws and Regulations in force, in particular (a) the verification of the technical, logical and organizational security measures implemented by Odaseva, (b) the verification of the Odaseva's data servers location where are hosted Principal Data, and (c) an analysis of the measures implemented to delete the Principal Data and to prevent any unauthorized disclosure of such Principal Data. The information as accessed by the Counterparty during the audit shall be subject to substantially the same terms and conditions as the "Confidentiality" section of the Agreement.

9.7 Transfer mechanisms for data transfers. The Standard Contractual Clauses will apply to any transfers of Personal Data made by Odaseva under this DPA from the EEA and/or their member states to its Sub-processors in countries which do not ensure an adequate level of data protection within the meaning of GDPR.

9.8 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 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 or, where [Section 9.2](#) applies, following a withdrawal of the HDS certifications, 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, unless prohibited by Data Protection Laws and Regulations. Upon a written request from the Counterparty, Odaseva will provide a written statement confirming such deletion or destruction. Until the Principal Data is deleted or destroyed, Odaseva shall continue to ensure compliance with this DPA.

9.9 Termination. Without prejudice to any provisions of GDPR, in the event that Odaseva is in breach of its obligations under the DPA, the Counterparty may instruct Odaseva to suspend the Processing of Personal Data until the latter complies with this DPA or until the Agreement is terminated. Odaseva shall promptly inform the Counterparty in case it is unable to comply with the DPA, for whatever reason.

The Counterparty shall be entitled to terminate this DPA insofar as it concerns Processing of Personal Data in accordance with this DPA if: (a) the Processing of Personal Data by Odaseva has been suspended by the Counterparty pursuant to this article and if compliance with this DPA is not restored within a reasonable time and in any event within thirty (30) days following suspension; (b) Odaseva is in substantial or persistent breach of this DPA or its obligations under GDPR; (c) Odaseva fails to comply with a binding decision of a competent court or the competent supervisory authority regarding its obligations pursuant to this DPA or to GDPR. Following termination of the DPA, Odaseva shall proceed according to [Section 9.8](#).

10. GENERAL PROVISIONS

10.1 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.

10.2 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.

11. DEFINITIONS

"Controller", "Data Subject", "Personal Data", "Process / Processing", "Processor" and "Sub-processor": all have the meanings set out in the GDPR, as amended or replaced from time to time.

“**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. For purposes of this definition, “**Control**” means direct or indirect ownership or control of more than fifty per cent (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 this DPA.

“**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.

“**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 Odaseva Technologies SAS, a company incorporated in France (registered no. 751 464 264 R.C.S.) having its registered office at 144, Avenue Charles de Gaulle, 92200 Neuilly-sur-Seine, FRANCE and which is a party to this DPA.

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

“**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 Odaseva. 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.

“**Standard Contractual Clauses**” or “**SCCs**” means the 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>.

LIST OF SCHEDULES

Schedule 1: Details of the Processing

Annex I: Data Processing Description

Annex II: [Technical and Organizational Security Measures](#)

Schedule 2: [List of Sub-processors](#)

SCHEDULE 1 – DETAILS OF THE PROCESSING

ANNEX I – DATA PROCESSING DESCRIPTION

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

A. LIST OF PARTIES

CONTROLLER:

Counterparty Entity Name:	As set forth in the Order Form
Address:	As set forth in the Order Form
Contact person’s name, position, and contact details:	As set forth in the Order Form
Activities relevant to the data processed:	Processing to carry out the SaaS Services pursuant to the Agreement entered into between Counterparty and Odaseva

PROCESSOR:

Odaseva Entity Name:	As set forth in the Order Form
Address:	As set forth in the Order Form
Contact person’s name, position, and contact details:	Data protection officer Data-privacy@odaseva.com
Activities relevant to the data processed:	Processing to carry out the SaaS Services pursuant to the Agreement entered into between Counterparty and Odaseva

B. DESCRIPTION OF PROCESSING

Categories of Data Subjects:	Counterparty's employees, trainees, applicants, former employees'	YES <input type="checkbox"/> No <input type="checkbox"/>
	employees of Counterparty's business partners (suppliers, service providers, freelancers, joint venture, temporary employment agency)	YES <input type="checkbox"/> No <input type="checkbox"/>
	Counterparty's authorized Users of the SaaS services	YES <input type="checkbox"/> No <input type="checkbox"/>
	Counterparty's clients, customers and/or prospects	YES <input type="checkbox"/> No <input type="checkbox"/>
	outsiders with whom the Counterparty has no business relationship (visitors, guests, interested parties)	YES <input type="checkbox"/> No <input type="checkbox"/>
Purpose(s) of the data processing:	performance of the SaaS Services pursuant to the Agreement.	
Categories of Personal Data:	<input type="checkbox"/> identification data (names, profile picture, email address, date and place of birth...) <input type="checkbox"/> personal life information (family status, number of children, lifestyle...) <input type="checkbox"/> professional life information (CV, training...) <input type="checkbox"/> traffic data (equipment ID, IP address, log in, password, time stamping information...) <input type="checkbox"/> economic and financial data (income, financial situation...) <input type="checkbox"/> location data (GPS/GSM data) <input type="checkbox"/> other: _____	
Sensitive data (if applicable) and applied restrictions or safeguards for sensitive data:	<input type="checkbox"/> biometric data for the purpose of uniquely identifying a natural person <input type="checkbox"/> genetic data <input type="checkbox"/> data concerning health <input type="checkbox"/> data concerning health of patients collected in France, under Section 9.2 <input type="checkbox"/> social security number <input type="checkbox"/> data revealing racial or ethnic origin <input type="checkbox"/> data revealing political opinions <input type="checkbox"/> data revealing religious or philosophical beliefs <input type="checkbox"/> trade union membership <input type="checkbox"/> data relating to criminal convictions and offences or related to security measures	
Health Data	SAFEGUARDS FOR 9.2 HEALTH DATA: <input type="checkbox"/> compliance of Counterparty with the enforceable reference systems of the PGSSI-S <input type="checkbox"/> HDS Certification [ADD DATE] of Odaseva for hosting activities No. [ADD NUMBERS] pursuant to Article R. 1111-9 of the French Public Health Code <input type="checkbox"/> HDS Certification [ADD DATE] of its Sub-processor Amazon Web Services for hosting activities No. [ADD NUMBERS] <input type="checkbox"/> HDS Certification [ADD DATE] of its Sub-processor Microsoft for hosting activities No. [ADD NUMBERS]	

Frequency of the processing:	Continuous
Nature of the processing:	Salesforce data management services, including the following operations: communication by transmission, download, anonymization, backup, storage, restore, replication, audit, analysis, search, updates, sampling, extraction, modification, deletion.
Duration of the processing	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:	The supervisory authority of the EU Member State in which the data exporter is established. See: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en
---	---