

Table of Contents

GENERAL CONDITIONS OF CONTRACT AND USE OF iNuba CLINIC.....	1
PRELIMINARY TITLE. CONTRACTUAL FRAMEWORK.....	1
TITLE I. PARTICIPANTS AND ACCESS.....	4
TITLE II. FUNCTIONAL CONTENT.....	5
TITLE III. FINANCIAL TERMS.....	9
TITLE IV. TERM AND TERMINATION.....	10
TITLE V. RULES OF USE AND LIABILITY.....	11
TITLE VI. FINAL PROVISIONS.....	13
ANNEX 1. DATA PROCESSING AGREEMENT.....	14
CHAPTER I. FRAMEWORK AND ARCHITECTURE OF ROLES.....	14
CHAPTER II. OBLIGATIONS OF THE PARTIES.....	15
CHAPTER III. FINAL PROVISIONS.....	18
APPENDIX A - IDENTIFICATION OF THE PARTIES.....	19
APPENDIX B - DESCRIPTION OF THE PROCESSING.....	19
APPENDIX C - TECHNICAL AND ORGANISATIONAL MEASURES.....	20
APPENDIX C BIS - AUTHORISED SUB-PROCESSORS.....	20
APPENDIX D - JOINT CONTROLLERSHIP (ART. 26 GDPR).....	21
ANNEX 2. SPECIFIC CONDITIONS OF WHITE LABEL MODE.....	22

GENERAL CONDITIONS OF CONTRACT AND USE OF iNuba CLINIC

Version 2.1 · Effective date: 7 August 2026

PRELIMINARY TITLE. CONTRACTUAL FRAMEWORK

1. Acceptance and scope

Access to and use of iNuba Clinic (hereinafter, the "Platform") entails acceptance of these General Conditions (the "Conditions") by the Customer and by each Professional operating under its account.

The electronic expression of agreement - registration checkboxes, re-acceptance screen or purchase process from the website - is documented in a verifiable and tamper-evident manner, recording the date, version number and digital fingerprint of the text, IP address and device, and binds both the Customer and the accepting Professional. Once a later version is published, a mandatory acceptance screen will be triggered after a courtesy period - seven (7) calendar days by default -, on the expiry of which access will be conditional on acceptance of the text in force.

iNuba reserves the right to deny or revoke access, at any time, to Professionals or Customers who breach the applicable Conditions.

2. Service provider

The Platform is owned by **3DHealthAI, S.L.**, with NIF B-40644445, with registered office at Polígono Industrial Los Vientos, C/ Levante, 1, 46119 Náquera (Valencia), Spain, and registered with the Registro Mercantil de Valencia (hereinafter, "iNuba"), in its capacity as an information society service provider under Ley 34/2002, of 11 July. Contact channel: info@inuba.com.

3. Glossary

Platform: web-based digital environment that iNuba makes available to the Customer and its Professionals so that they can provide their End Users with health monitoring, follow-up and management services.

Customer (or Company): health professional or sector entity that contracts the Platform and under whose company account its use is organised.

Account Holder (or Owner): Professional who owns the Customer's company account, the only person entitled to contract, change the plan, pause and cancel the account.

Professional: any natural person who, on behalf of the Customer, uses the Platform to carry out their work, whatever their profile (administration, management, nutrition, training or health). The Professional does not have Customer status, without prejudice to the Account Holder holding both.

End User (or connected client): natural person using the iNuba App who is linked to the Customer, irrespective of the access route. This is the only category of linked person the Platform recognises: there are no intermediate categories and no links of reduced scope. Any reference to "patient",

"connected client" or "App user" is to be understood as referring to the End User.

Service: the set of services iNuba provides through the Platform.

iNuba Hardware: iNubaBox booth, iNuba Totem device and other body capture equipment developed or distributed by iNuba.

iNuba AI: artificial intelligence systems used by iNuba to produce nutrition and training proposals and to assist in the execution of protocols, on the terms of section 9.

White Label Mode: contractual arrangement under which the Customer distributes the iNuba App under its own brand among its customers, in accordance with Annex 2.

White Label App: the iNuba App customised with the Customer's brand, the ownership, infrastructure, database and actual provision of which belong exclusively to iNuba.

Access API: technical interface that iNuba provides to the White Label Mode Customer in order to report the registrations of its customers and their access status.

Parties: iNuba and the Customer, including its Account Holder and its Professionals.

4. Subject matter, nature and plans

These Conditions govern access to, navigation of and use of the Platform, as well as the use of the Services provided through it. Certain services may be subject to specific conditions that replace, supplement or amend this text.

Nature. The Platform is a management tool. It does not provide healthcare services and does not displace the clinical judgement of the Customer, who declares that it holds the legal authorisation required to carry out its activity and is solely answerable for the care decisions it takes.

White Label Mode. The Customer may additionally contract the distribution of the iNuba App under its own brand, governed by the specific conditions of Annex 2. Registration on the Platform and acceptance of this document are the single, standardised route for contracting that mode, irrespective of how intensively the Customer uses the remaining services.

5. Contracting parties

These Conditions are entered into by iNuba, on the one hand, and the Customer, on the other. The Customer's Professionals who register on the Platform may also acquire the status of Party. They will jointly be referred to as the "Parties".

TITLE I. PARTICIPANTS AND ACCESS

6. Participant profiles

There are different types of participant depending on their relationship with the Platform, using the terminology of the software itself:

- **Customer (or Company):** the party that contracts the Platform and under whose company account its use is organised.
- **Account Holder (or Owner):** Professional who owns the company account, the only person entitled to contract, change the plan, pause and cancel.
- **Professional:** the person who uses the Platform to carry out their work on behalf of the Customer. Professionals are organised into internal profiles with differentiated powers, in accordance with section 10.
- **End User:** person linked to the Customer through the iNuba App who receives its services. They are not a party to these Conditions, and their relationship with iNuba is governed by the General Conditions of Use of the iNuba App.

The Account Holder and each Professional undertake to: (i) declare that they are of legal age and have legal capacity; (ii) provide only true, accurate and complete data about their identity and standing; and (iii) be answerable for the authenticity and currency of that data. iNuba does not verify the professional registration or the professional status of the Professionals. The supply of false, inaccurate or incomplete data, or the existence of well-founded indications allowing its truthfulness to be questioned, will entitle iNuba to deny present or future access.

7. Registration and verification

7.1. Direct registration. This requires a name, email address and password - a minimum of eight (8) characters with a lower-case letter, an upper-case letter and a digit or symbol -, as well as acceptance, through specific

checkboxes, of these Conditions, of the Privacy Policy and of the data processing regime in Annex 1. The email address is verified by means of a six (6) digit code; without verification it is not possible to log in. Registration automatically creates the Customer's company account. The tax details - company name, NIF or CIF, address and billing email address - are completed under User → Billing before the subscription is purchased.

7.2. Purchase from the website. The Platform may be purchased from the public website by providing an email address and a name and expressly accepting the conditions; the account is created when payment is confirmed, and the acceptance is recorded.

7.3. Registration through an authorised distributor. Registration may originate through an authorised distributor, which passes the Account Holder's contact details to iNuba; in that case, the plan and the limits of the trial period may differ from the standard ones.

The procedures above may evolve, and the foregoing indications are purely illustrative. Queries: support@inuba.com.

TITLE II. FUNCTIONAL CONTENT

8. Platform features

The Platform makes available to the Customer and its Professionals only the features listed below. Their actual availability may depend on the plan contracted and on the Professional's profile. Any feature not included in this list falls outside the subject matter of the contract, and its existence may not be presumed nor its implementation required.

8.1. Direct connection with the iNuba Hardware and analysis of the information captured. Direct integration with the iNuba Hardware and detailed consultation of all the information that equipment generates in respect of the Customer's End Users: body and body composition measurements, bioimpedance, images and three-dimensional reconstruction, thermography and skin assessment, with their analytical detail and their evolution over time.

8.2. End User management. Invitation of End Users - who accept the link through an invitation sent to their email address -, consultation of their record and history, editing, reassignment within the company and unlinking. Once the link is completed, the Professional accesses the whole of the End User's clinical information to the extent determined by their profile, and

there are no linking categories of reduced scope. The Customer warrants that it has a legal basis for providing the contact details of the persons it sends invitations to.

The Professional may add files to the End User's profile, with a title, category and tags, warranting that they have the authorisation of the data subject and that the content complies with the legislation in force; iNuba is not answerable for the truthfulness or the content of the documents added. The addition of files unrelated to the Services, harmful to third party rights or of unlawful or offensive content is prohibited. Where the assignment of an End User to a Professional ceases, that Professional will lose access to their information, which will remain blocked and will only be accessible upon request by a competent authority, after notifying iNuba and by means of audited access.

8.3. Monitoring of health parameters through wearables.

Synchronisation and consultation of the biometrics, activity and habits that End Users provide from wearable devices and from the health platforms on their device, following their evolution as the data is taken in.

8.4. Recording of health variables. Recording and consultation of the End User's health variables - body measurements, biomarkers, clinical and laboratory parameters and daily record of habits -, with traceability of their origin (the End User, the iNuba Hardware, a wearable or the Professional).

8.5. Nutrition plans produced with iNuba AI. Generation of dietary guidance adjusted to the End User's goals and recorded needs, by means of iNuba's artificial intelligence systems, subject to section 9. The Professional may review, amend, replace or discard the proposal before assigning it.

8.6. Training plans produced with iNuba AI. Generation of physical conditioning programmes adjusted to the End User's goals and progress, by means of iNuba's artificial intelligence systems, subject to section 9 and with the same power of review by the Professional.

8.7. Automated health protocols. Configuration of sequences of actions - sending questionnaires, requesting measurements, reminders and assignment of plans or content - triggered automatically on the basis of the End User's profile and of the activity they record. The design, parameterisation and supervision of each protocol are a matter for the Customer, who is answerable for their conformity with the lex artis and with

the applicable healthcare legislation. Protocols do not take decisions with legal or similarly significant effects concerning the End User.

8.8. Custom questionnaires. Creation, editing and assignment of questionnaires and forms adapted to the Customer's operations and follow-up, with consultation of their status - pending, in progress, completed or cancelled -, of the individual answers and of their aggregated statistics.

8.9. Range-based alerts. Definition of margins for any recorded variable and automatic generation of notices when the value exceeds them. Alerts rely on rules that the Customer itself configures and serve an informational function: they do not constitute a diagnosis, a clinical assessment or an automated decision with legal effects, and their interpretation and any resulting action are a matter for the Professional.

8.10. Segments. Creation of automatic lists of End Users according to categories and filters defined by the Customer, referring exclusively to the End Users of its own company, in order to automate the assignment of alerts, questionnaires, protocols and follow-ups.

8.11. Follow-up app for End Users. The Customer's End Users have the iNuba App, from which they consult their information, their variables, their plans, their questionnaires and their alerts, and from which they receive the operational and care-related notifications arising from the Customer's activity. The relationship between iNuba and the End User is governed by the General Conditions of Use of the iNuba App and by its Privacy Policy.

8.12. Billing and legal centre. Consultation of the account's billing (plan, seats, tax details and payment portal) and access to the legal centre, with the documents in force and the history of the Professional's acceptances and consents.

9. Artificial intelligence: scope, limits and liability

9.1. The features in sections 8.5 and 8.6, as well as certain support functions of the protocols in section 8.7, make use of artificial intelligence systems. iNuba expressly discloses this in compliance with the transparency obligations of Regulation (EU) 2024/1689 of 13 June 2024.

9.2. Nature of the output. The systems produce **proposals of an indicative nature** addressed to the Professional. They do not issue diagnoses, do not set out drug treatment and do not prescribe any therapy. The Platform is not a medical device and is not marketed as such.

9.3. Human oversight. Every proposal requires validation by the Professional before it is assigned to the End User. The Customer undertakes to put that oversight in place and to prevent the automatic assignment of proposals without professional intervention. Consequently, there are no decisions based solely on automated processing within the meaning of Article 22 GDPR.

9.4. Liability. The Customer assumes sole liability arising from the professional judgement it applies to the proposals generated, as well as for their suitability for each End User in view of their circumstances - medical conditions, pregnancy, breastfeeding, allergies, intolerances or ongoing medication. iNuba is answerable for the systems operating as described, without guaranteeing the absolute accuracy of the output or its suitability for a specific case.

9.5. Data used. The information used to generate the proposals and the conditions for its possible use to train or improve the systems are governed by Annex 1 and by the iNuba App Privacy Policy.

9.6. Providers. The systems run on iNuba infrastructure or on third-party services engaged as Sub-processors, contractually bound not to use the information to train their own models and to delete it once the processing is complete. Their up-to-date list appears in Annex 1.4.

10. Team, profiles and seats

Access control operates through profiles with differentiated powers: the administration and management profiles cover the End Users of the whole company; the care profiles - nutrition, training and health - cover the End Users of the company or exclusively those assigned to them, according to the configuration the Customer itself establishes for each Professional.

The number of registered Professionals is limited according to the plan contracted; once it expires, access to the features is blocked. The Customer will assign profiles in accordance with the principle of least privilege and will revoke the access of staff who have left. The termination of a Professional revokes their access immediately and reassigns their End Users to the Account Holder, with the information they had added remaining in the company account.

11. Support

The Platform includes a help button that opens WhatsApp with a predefined message addressed to iNuba support; its use entails the processing of the communication by Meta in accordance with its terms. The Professional will refrain from including End User data in that channel. There is no messaging integration with End Users; its possible future activation will be communicated and documented beforehand.

TITLE III. FINANCIAL TERMS

12. Subscription plans

The Platform is offered in three plans - Basic, Pro and Platinum -, with monthly or annual billing, the latter at a discount, and tiered prices depending on the number of End Users contracted and the limits published during the purchase (number of professionals, storage, linked End Users and active protocols or plans). The plan limit counts all linked End Users, and there are no categories exempt from counting.

Trial period. Seven (7) days from registration, with no need to provide a card, with the configuration indicated at registration itself. If it ends without a purchase, access is blocked, and no automatic charge whatsoever is made.

The content of each plan may be modified by giving the Customer thirty (30) days' prior notice. Such modifications will not give rise to compensation, without prejudice to the Customer's right to cancel with effect at the end of the current period.

13. Price, taxes and payment method

13.1. General regime. The Customer will pay, at any given time, the price of the plan and of the services concerned, as shown on screen. Amounts are expressed in euros (€) excluding VAT, and the applicable taxes are calculated automatically during payment according to the Customer's tax jurisdiction.

13.2. Payment of the subscription. This is handled through Stripe, with payment in advance and automatic renewal for equal periods unless previously cancelled. iNuba does not keep card details. Invoices are issued and made available through the Stripe customer portal.

13.3. Plan changes. Increases - more seats or a higher plan - take effect immediately with pro rata charging; reductions are scheduled for the end of

the current period and may be cancelled before they take effect. Reductions below the number of active clients or professionals are not permitted.

14. Non-payment

Where a subscription payment fails, the following staged process will apply, communicated by email to the Account Holder:

- **Day 0:** notice of the incident; access is maintained.
- **Day 10:** reminder.
- **Day 15:** suspension of the account with access blocked, reversible by payment at any time; the information remains intact.
- **Day 30:** final notice.
- **Day 37:** opening of the cancellation process (termination pending).
- **Day 67:** closure of the account, with blocked retention for the legal periods and subsequent anonymisation in accordance with section 16.

Payment verified before closure reactivates the account with all of its information intact.

TITLE IV. TERM AND TERMINATION

15. Cancellation, pause and termination

15.1. Voluntary cancellation. The Account Holder may cancel the subscription whenever they see fit from the Platform, by means of reinforced confirmation. Cancellation takes effect at the end of the period already paid for, with no right to a refund of the amounts paid and with the Service being maintained until that date. The account then enters a grace period of thirty (30) days with full access, intended, among other purposes, for obtaining the necessary information; once that period has elapsed, the account is closed in accordance with section 16.

15.2. Voluntary pause. The Account Holder may pause the account for a period of between one (1) and six (6) months, with no charge, with the Platform being blocked reversibly. If the pause expires without reactivation, it will become a cancellation with its corresponding grace period.

15.3. Termination by iNuba. iNuba may suspend access or terminate the contract in the event of a breach by the Customer of its contractual obligations - including the non-payment in section 14 -, fraud, use contrary to these Conditions or a request by an authority, with reasonable prior notice

save in cases of urgency, and remains free to claim the damages arising from the breach.

16. Account closure and destination of the information

Once closure has occurred, whether voluntary or due to non-payment: (i) the Professionals are deregistered; (ii) the End Users are unlinked, keep their app working normally and are informed of this; and (iii) the information is blocked and kept for the legal periods - as a general rule, five (5) years for that of the End Users, four (4) years for that of the Professionals and six (6) years for that of the Account Holder -, after which the personal data of End Users and Professionals is definitively and irreversibly anonymised.

Restoration. Once closure has taken place, the account may be restored during the retention period by requesting it from iNuba through the usual channel, subject to the re-acceptance of the texts in force. Anonymisation is irreversible.

TITLE V. RULES OF USE AND LIABILITY

17. Continuity of the Service

The Platform is available to those who have an internet connection. iNuba will make all reasonable efforts to sustain its permanent availability, seeking maximum continuity apart from planned maintenance. Nevertheless, since access is channelled through an internet connection, its quality and availability may be affected by circumstances beyond iNuba's control, and iNuba is not answerable for the unavailability resulting from them.

18. Standard of care required

It is for the Customer and its Professionals to make correct use of the Platform, providing truthful and lawful information. iNuba will not be answerable for the consequences arising from a breach of these Conditions or for the damage caused to the Professional's computer system as a result of: (i) the presence of viruses on their device; (ii) a malfunction of the Platform; or (iii) the use of out-of-date versions.

19. Prohibited conduct

iNuba retains the power to cancel the access of the Professional or of the Customer in the event of a breach of the obligations assumed or of a use

contrary to these Conditions, to the Privacy Policy or to the good faith practices of the sector. The Customer and each Professional undertake to:

- Enter truthful information and keep it up to date.
- Use End User information exclusively for the provision of their professional services, in full compliance with data protection, healthcare and professional secrecy legislation, and obtaining from End Users the consents their activity requires, without the Platform's tools displacing that responsibility.
- Refrain from entering third party data without standing to do so and from adding unlawful or offensive files or files harmful to the rights of others.
- Not use the Platform to collect personal data of other users or to carry out timesharing operations or to provide access to third parties.
- Refrain from reverse engineering or actions aimed at developing an identical or similar platform.
- Not subject the Platform to loads intended to destabilise it, including denial of service attacks.
- Not remove or tamper with iNuba's intellectual or industrial property notices.
- Not cause damage to the systems of iNuba, of its providers or of third parties, nor introduce viruses or other harmful elements.
- Safeguard their credentials and those of their team, and inform iNuba of any risk to security.
- Pay the agreed prices.

20. Linked third-party resources

These Conditions do not extend to the links, applications and services of third parties accessible from the Platform - among others, Stripe, Google and WhatsApp/Meta. The Customer and its Professionals accept being subject to their respective terms and policies. iNuba is not answerable for their content or for their security measures.

21. Liability

iNuba does not guarantee the uninterrupted availability of the Platform, although it will use its best diligence to ensure its regularity and correct operation. iNuba assumes no liability for harm arising from disconnections, interference or interruptions, nor for viruses or other harmful elements, nor

in respect of the errors or omissions in the content that the Customer or its Professionals add, nor of the plans, protocols and programmes they implement for their End Users, for which the Customer is solely answerable.

iNuba's total liability towards the Customer, save for wilful misconduct or gross negligence, is limited to the amounts actually paid by the Customer in the twelve (12) months preceding the triggering event, and in no case extends to loss of profit. The Customer will hold iNuba harmless against claims by End Users or third parties arising from the Customer's breach of its legal or contractual obligations.

22. Force majeure

The Parties will be released from the non-performance of their obligations where it is due to causes reasonably beyond their control, such as - without limitation - fires, floods, epidemics and pandemics, strikes, labour disputes, shortage or unavailability of energy, unavailability of communications networks, accidents, wars, embargoes, blockades, riots or insurrections.

TITLE VI. FINAL PROVISIONS

23. Intellectual and industrial property

The Customer and its Professionals acknowledge and accept that all industrial and intellectual property rights over the Platform and over the elements added by iNuba - including, by way of example, the "look and feel", trade marks, logos, texts, images, designs, databases, software, artificial intelligence models and their output, navigation architecture and source code - belong exclusively to iNuba or to lawful third party assignors.

The Customer and its Professionals are granted a non-exclusive and non-transferable licence, limited to the use of the Platform within their professional activity for the term of the contract. The Customer retains ownership of the content and data it adds, granting iNuba the licences essential to operate the Service and the authorisations in Annex 1.

24. Personal data protection

The processing of the personal data of the Account Holder and of the Customer's Professionals is governed by the iNuba Clinic Privacy Policy. The processing of End User data is governed by Annex 1 - Data Processing Agreement -, which forms part of these Conditions, and, as regards the data for which iNuba is the Data Controller, by the iNuba App Privacy Policy.

25. Notices

Notices between the Parties will be deemed effective when made through the Platform or through the email address designated by each of them. The Customer designates its Account Holder as the point of contact and undertakes to keep their email address operational. Price changes will be communicated with a minimum of thirty (30) days' notice and will apply from the following renewal.

26. Revision of these Conditions

iNuba may revise this text and its Annex 1. Successive versions will be published stating their effective date and digital fingerprint, and re-acceptance will be obtained in accordance with section 1. The version history will remain available at inuba.com/legal.

27. Governing law and jurisdiction

These Conditions are subject to Spanish law. The Parties, expressly waiving any other jurisdiction to which they may be entitled, submit to the courts and tribunals of Valencia, save for any mandatory rule to the contrary.

ANNEX 1. DATA PROCESSING AGREEMENT

CHAPTER I. FRAMEWORK AND ARCHITECTURE OF ROLES

1. Subject matter and applicable legislation

For the purpose of governing the processing of personal data covered by this agreement, both Parties agree to enter into it, and it will be subject to Regulation (EU) 2016/679 of 27 April 2016 ("GDPR"), to Ley Orgánica 3/2018, of 5 December ("LOPDGDD"), to its implementing legislation and to the provisions set out below.

2. Terminology

The terms used in this agreement (the "Agreement") will have the meaning attributed to them by Article 4 GDPR. The respective functions, duties and obligations of the Data Controller and the Data Processor are set out in the Agreement itself. The identification of the Parties according to the role assumed appears in Appendix A.

3. Allocation of roles in the iNuba ecosystem

(a) iNuba as Data Controller, in respect of the information generated automatically by the End User - App, iNuba Hardware, wearables and App questionnaires -, which the End User consents to directly with iNuba, as well as of the data of the Customer's Account Holder and Professionals.

(b) Customer as Data Controller and iNuba as Data Processor, in respect of the information that the Customer and its team manually add to the Platform about their End Users: clinical record, observations, variables recorded by the Professional, questionnaires designed by the Customer and their answers, protocols configured, plans assigned, alert thresholds, segments and files. This processing engagement is governed by Chapters II and III.

(c) Joint controllership, in respect of those processing operations in the ecosystem whose purposes and means are determined jointly by the Parties, governed by Appendix D.

CHAPTER II. OBLIGATIONS OF THE PARTIES

4. Description of the processing

The details of the processing, in particular the categories of data and the purposes pursued on behalf of the Data Controller, are set out in Appendix B.

5. Obligations of the Data Processor

5.1. Instructions. The Data Processor will process the data following only documented instructions from the Data Controller, with this Agreement and the configuration of the Platform constituting the main instruction, unless Union or Member State law requires otherwise, in which case it will inform the Data Controller before the processing, unless legally prohibited on important grounds of public interest. The Data Processor will immediately inform the Data Controller if, in its opinion, an instruction infringes the GDPR or the applicable legislation.

5.2. Purpose limitation. The Data Processor will process the data only for the specific purposes of the Agreement, save for additional documented instructions.

5.3. Duration. The processing will last for the period indicated in Appendix B.

5.4. Security. The Data Processor will implement, as a minimum, the technical and organisational measures in Appendix C, aimed at protecting the data against personal data breaches leading to its destruction, loss, alteration, unauthorised disclosure or unlawful access. Access will be granted only to strictly necessary personnel, ensuring that the authorised persons have committed themselves to confidentiality or are under an equivalent statutory obligation.

5.5. Special categories. The processing engagement covers the processing of special category data - health data -, and the Data Processor will therefore apply the additional restrictions and safeguards provided for in this Agreement and in Appendix C.

5.6. Demonstrating compliance and audits. Both Parties must be in a position to demonstrate compliance with these clauses. The Data Processor will promptly deal with the Data Controller's queries and will make available to it all information necessary to demonstrate compliance, allowing for and contributing to audits. The Data Controller will give one (1) month's notice of its intention to audit; the audit will be carried out during ordinary working hours, without substantially disrupting the Data Processor's operations and with access limited to the data processed on the Data Controller's behalf, with a maximum of one audit per calendar year save in the event of demonstrable non-compliance. The auditor will be bound by confidentiality. The results will be made available to any supervisory authority that requests them. iNuba additionally has a tamper-evident record of consents and acceptances that can be exported for inspection purposes.

5.7. Sub-processors. The Data Processor may subcontract ancillary providers without prior express authorisation, provided that they assume identical data protection obligations. The Sub-processors authorised at the time of contracting are listed in Appendix C bis. The Data Processor will give a minimum of fifteen (15) days' notice of the addition or replacement of Sub-processors, and the Data Controller is entitled to object on justified grounds; in that case, the Parties will seek a reasonable solution, including waiving the affected service or terminating the contract without penalty. At the Data Controller's request, the Data Processor will provide a copy of the contract entered into with its Sub-processors, retaining in all cases full liability for their compliance.

5.8. International transfers. Any transfer to a third country or international organisation will be carried out on the basis of documented

instructions from the Data Controller or in order to comply with a legal requirement, in accordance with Chapter V GDPR. The Data Controller accepts that, where a Sub-processor carries out activities involving an international transfer, compliance may be ensured through the standard contractual clauses adopted by the Commission (Art. 46(2) GDPR) or another valid mechanism, provided that its conditions are met.

5.9. Assistance to the Data Controller. Taking into account the nature of the processing, where the Data Processor receives a request to exercise rights relating to data processed on behalf of the Data Controller, it will forward it without delay and will assist the Data Controller in handling it within a maximum period of one (1) month, with the Data Controller being responsible for deciding the requests arising from its own processing. The Data Processor will likewise assist the Data Controller with: (i) impact assessments where processing may entail a high risk; (ii) prior consultations with the supervisory authority; (iii) the accuracy and updating of the data, informing it without delay if it becomes aware that the data is inaccurate or out of date; and (iv) the obligations of Article 32 GDPR, to the extent set out in Appendix C.

5.10. Personal data breaches. Where a breach of the security of the data processed on behalf of the Data Controller occurs, the Data Processor will notify it without undue delay and, in any event, within twenty-four (24) hours of becoming reliably aware of it, cooperating with and assisting the Data Controller in complying with Articles 33 and 34 GDPR.

6. Authorisation of further uses

The Customer, in its capacity as Data Controller of the information described in clause 3(b), expressly authorises iNuba to:

- (a)** apply pseudonymisation and anonymisation techniques to that information;
- (b)** use the pseudonymised data to improve the Platform, to develop new features, to train and improve the artificial intelligence systems described in section 9 of the Conditions, to produce statistics and to carry out scientific research, with the safeguards of Article 89 GDPR; and
- (c)** use and share with third parties irreversibly anonymised datasets - which cease to be personal data - for research, statistical or health product and service development purposes.

Conditions. (i) Uses making use of data capable of identifying the End User will additionally require the End User's consent, obtained through the App; (ii) the activation of the sharing with third parties is subject to a prior impact assessment and to technical anonymisation controls with a minimum aggregation threshold; (iii) the Customer may revoke this authorisation whenever it sees fit before the Data Protection Officer (dataprotection@inuba.com), and iNuba will stop including its information in new processing operations, with no effect on information already anonymised, which is irreversible by design; and (iv) the information of minors is excluded from the sharing with third parties.

7. Access by iNuba staff (super-administration)

The Customer is informed of and accepts that authorised iNuba staff, under a super-administration profile, have cross-cutting technical capabilities over the whole of the Platform, apart from the per-company isolation applicable to the Customer's Professionals. Those capabilities include support and maintenance, the auditing of consents, the handling of rights requests, the administration of the Service and, technically, read and write access to End User information, including information of a clinical nature. Such access is limited to authorised staff, is subject to confidentiality, to the measures in Appendix C and to the Data Controller's instructions, and forms part of the processing engagement.

CHAPTER III. FINAL PROVISIONS

8. Non-compliance and termination

Without prejudice to the provisions of the GDPR, where the Data Processor fails to comply with its obligations, the Data Controller may instruct it to suspend the processing until it complies, or terminate the contract; the Data Processor will inform the Data Controller without delay if it is unable to comply with these clauses. The Data Controller may terminate the contract as regards the processing where: (a) the Data Processor substantially or persistently breaches these clauses or its obligations under the GDPR; or (b) it fails to comply with a binding decision of a court or of a supervisory authority. The Data Processor may terminate it where, the Data Controller having been informed that its instructions infringe the legislation, it insists on them.

9. Destination of the data on termination

Once the Service has ended, the Data Processor will, at the Data Controller's choice, delete or return the data processed on its behalf, without prejudice to the blocked retention required by law (section 16 of the Conditions). The return will be made in a structured, commonly used format, within the period agreed by the Parties in view of the volume and complexity. Once the legal retention periods have elapsed, the data will be irreversibly deleted or anonymised.

APPENDIX A - IDENTIFICATION OF THE PARTIES

Data Controller: the Customer - professional or entity holding the company account -, in respect of the information that it and its team add about their End Users.

Data Processor: 3DHealthAI, S.L. (iNuba), NIF B-40644445, Polígono Industrial Los Vientos, C/ Levante, 1, 46119 Náquera (Valencia), Spain. Data Protection Officer: dataprotection@inuba.com.

Independent Data Controller: iNuba, in respect of the information self-generated by the End User and of the data of the Customer's Account Holder and Professionals, matters that fall outside this processing engagement.

APPENDIX B - DESCRIPTION OF THE PROCESSING

Data subjects: End Users linked to the Customer.

Categories of data: identification and contact data; health data, as special category data - clinical record (history, allergies and medication), observations, variables and measurements, iNuba Hardware results, biometrics from wearables, questionnaire answers, nutrition and training plans assigned, protocols executed and alerts generated -; images and photographs provided; documents and files added by the Customer.

Operations: collection, recording, structuring, storage, consultation, disclosure to the Data Controller itself and to the End User through the App, backup, blocking, deletion and anonymisation, together with the ancillary operations in clauses 6 and 7.

Purpose: the provision of the Platform to the Data Controller, as well as the further uses authorised in clause 6.

Duration: the term of the contract, extended by the legally required blocked retention periods.

APPENDIX C - TECHNICAL AND ORGANISATIONAL MEASURES

Organisational measures: appointment of a Data Protection Officer; record of processing activities; least privilege policy and confidentiality of staff; training; personal data breach management procedure with notification to the Data Controller within twenty-four (24) hours; tamper-evident record of consents and acceptances, exportable for audit purposes; procedure for handling rights requests.

Technical measures: encryption of communications (TLS); access control by profile and seat with mandatory email verification; logical isolation per company (multi-tenancy); audit log of access to blocked records and of lifecycle events; verification of signatures in payment notifications; pseudonymisation in analytics processes and in the flows directed to artificial intelligence systems; daily backups on a separate server within the European Union; hosting in the European Union (France); blocking and anonymisation on the expiry of the retention periods in accordance with internal procedures.

APPENDIX C BIS - AUTHORISED SUB-PROCESSORS

Sub-processor	Service	Location
Amazon Web Services EMEA SARL	Hosting and storage (Paris region)	EU (France)
OVHcloud	Server infrastructure	EU (France)
Stripe Payments Europe, Ltd.	Payment processing and subscription billing	EU (Ireland); transfers with safeguards
Amazon SES	Transactional email	EU
Google Ireland Ltd. (Firebase Cloud Messaging)	Delivery of notifications to the End User's App; receives the device identifier and the content of the notification	EU / US with safeguards
Artificial intelligence	Generation of nutrition and training proposals, without using the	Depending on the

Sub-processor	Service	Location
model provider	information to train its own models and with deletion once the processing is complete	provider; transfers with safeguards

The up-to-date list, naming the artificial intelligence model provider, its location and its safeguards, is published at inuba.com/legal.

APPENDIX D - JOINT CONTROLLERSHIP (ART. 26 GDPR)

1. Scope

The Parties jointly determine the purposes and means of the following processing operations: (i) the management of the registration and of the link between the End User and the Customer; (ii) the End User's activity history originating in the App, in wearables, in the iNuba Hardware or in the clinic; and (iii) the synchronisation of information between the App and the Platform.

2. Obligations

(a) Information to data subjects. This is provided through the iNuba App Privacy Policy, which describes the essential terms of this agreement, and through the Customer's own information. The essential terms are made available to data subjects who request them.

(b) Point of contact. iNuba acts as the single point of contact for data subjects (dataprotection@inuba.com), without prejudice to their right to exercise their rights against either Party.

(c) Handling of rights. Each Party will decide the requests relating to the information for which it is the Data Controller, providing mutual assistance without delay.

(d) Security and breaches. Each Party will implement appropriate measures within its own sphere, notifying the other without undue delay - and, in any event, within twenty-four (24) hours - of the breaches affecting the jointly controlled processing operations, and coordinating the notifications to the authority and to the data subjects.

(e) Cessation. Once the relationship has ended, each Party will keep the information within its sphere in accordance with the legal periods, applying the blocking and anonymisation provided for.

ANNEX 2. SPECIFIC CONDITIONS OF WHITE LABEL MODE

These specific conditions apply exclusively to Customers that contract White Label Mode and prevail, as regards that mode, over the general conditions, which continue to apply to everything not provided for here - including the clauses on continuity, liability, force majeure, intellectual property, notices, revision and governing law.

1. Subject matter and operating model

1.1. iNuba grants the Customer the non-exclusive and non-transferable right to distribute the White Label App among its customers under its own brand for the term of the mode. Customisation is limited to the brand elements agreed; the White Label App is, for all purposes, the iNuba App.

1.2. The Customer manages the commercial relationship with its customers: acquisition, registration, prices, billing, collection and the decision on maintaining or suspending each one's right of access, which it reports to iNuba through the Access API. The Customer is answerable for its own commercial conditions vis-à-vis its customers, which it will obtain and keep through its own channels; iNuba is not a party to that relationship.

1.3. iNuba provides the app service to the End Users: it operates the White Label App, its infrastructure and its database, and processes the information generated in it as Data Controller, in accordance with clause 5 of this Annex. On first access, each End User accepts the General Conditions of Use and the Privacy Policy of the iNuba App, which inform them that the service is provided by iNuba under the Customer's brand.

1.4. The suspension of the right of access reported through the API entails the suspension of the End User's access to the White Label App; their information remains in the account in accordance with the iNuba App Privacy Policy.

2. Access API, brand and publication

2.1. iNuba provides the Customer with Access API credentials, which are personal and non-transferable and which the Customer must safeguard, having to notify any compromise of them immediately. Through the API the Customer reports the identification data needed for registration - name, email address, identity document and date of birth -, the access status and, where it holds them and they are necessary for the provision of the service, the End User's health profile data - sex, ethnic origin, declared conditions, height and weight -, warranting their accuracy and the availability of a legal basis for disclosing them. The Customer will not use the API for other purposes and will not attempt to access other information in the app.

2.2. The Customer licenses iNuba, on a non-exclusive and royalty-free basis, to use its brand solely for the purposes of customising, publishing and promoting the White Label App for the term of the mode. Publication in the app stores will comply with the policies of those platforms, and the app's legal information will identify 3DHealthAI, S.L. as owner and provider in accordance with Ley 34/2002.

2.3. All intellectual and industrial property rights over the app, its code, design, "look and feel" - save for the Customer's brand -, databases and content belong exclusively to iNuba.

3. Specific obligations of the Customer

The Customer undertakes to: (a) inform its customers, clearly and before contracting, that the app service is provided by iNuba (3DHealthAI, S.L.) under its brand; (b) maintain its own commercial conditions that are lawful and compliant with consumer legislation; (c) report through the API only accurate data of persons with a valid relationship; (d) refrain from requesting, collecting or attempting to access the health information, images or any other data generated by End Users in the app, save for that which iNuba discloses to it in accordance with clause 5.4; (e) refrain from statements attributing to itself the ownership of the app or of the processing; and (f) pay the consideration for the mode in accordance with the commercial offer accepted.

4. Financial conditions, term and termination

4.1. The consideration for White Label Mode - licence, price per active user, revenue share or another model -, its frequency and its term are those of the

commercial offer accepted by the Customer at the time of contracting, which is recorded together with the acceptance of this document. For matters not provided for, the general conditions on prices, non-payment and cancellation apply.

4.2. Effects of termination. (i) The Customer will cease distribution and iNuba will cease using its brand; (ii) the Access API will be deactivated; and (iii) the End Users will be informed and may continue using the standard iNuba app with the same account, or terminate their account in accordance with the General Conditions of Use of the iNuba App, with their information remaining under iNuba's responsibility. Termination does not affect iNuba's relationship with the End Users or the processing operations in clause 5 of this Annex.

5. Data protection in White Label Mode

5.1. Independent Data Controllers. In this mode, each Party is an independent Data Controller for its respective processing operations: the Customer, in respect of its customers' data in the commercial relationship (acquisition, contracting, billing and payment control); iNuba, in respect of the End Users' information in the app (account, health data, images and usage), in accordance with the iNuba App Privacy Policy. The processor regime in Annex 1 will only apply if, in addition, the Customer uses the Platform's features to add information about its End Users.

5.2. Disclosure through the API. The disclosure of the identification data and of the access status is a disclosure between Data Controllers, relying on the performance of the respective contracts with the data subject (Art. 6(1)(b) GDPR). The Customer will report that disclosure in its own data protection information.

5.3. Acknowledgement of iNuba's processing. The Customer expressly acknowledges and accepts that iNuba, as an independent Data Controller, processes the information generated by End Users in the app in accordance with its Privacy Policy, including storage for the service, the history and progress tracking; the production of statistics using anonymised data; and, with the End User's consent where required, the training and improvement of its technology and the sharing of anonymised datasets. The Customer acquires no right whatsoever over that information or over the datasets, statistics, models or outputs derived from it, and will refrain from interfering in the data protection relationship between iNuba and the End Users.

5.4. Access limits. As a general rule, the Customer will not receive health data, images or any other data generated by End Users in the app, and iNuba will limit itself to disclosing the account status information - effective registration and termination - needed to manage access. However, where the Customer is also an occupational health service or a healthcare entity and the scans are performed within its activity, iNuba will disclose to it the scan results of its End Users - body measurements, body composition, temperatures and thermographic images -, which the Customer will process as an independent Data Controller and in accordance with the legal basis applicable to it. Any additional flow will require a specific written agreement and, where appropriate, the End User's consent.

5.5. Assistance and personal data breaches. Each Party will handle the data subject rights relating to its own processing operations, with reasonable mutual assistance, notifying the other without undue delay - and, in any event, within twenty-four (24) hours of becoming aware of it - of the personal data breaches affecting the information disclosed between them. These obligations survive termination for as long as that information is kept.