

Table of Contents

iNuba APP PRIVACY POLICY.....	1
Summary.....	1
1. Data Controller.....	2
2. When this text applies and who decides what.....	2
3. What information we process.....	3
4. Purposes and legal bases.....	5
5. Artificial intelligence.....	7
6. Your images and your data: ordinary operation and the decisions that are yours.....	7
7. Who else accesses your information.....	9
8. Data location and international transfers.....	10
9. How long we keep your information.....	11
10. What you can require from us.....	11
11. Security measures.....	12
12. Minimum age.....	12
13. Updates to this text.....	12

iNuba APP PRIVACY POLICY

Version 3.1 · Effective date: 7 August 2026

Summary

This summary does not replace the full text, but sets out the essentials up front:

- **Who decides about your information.** 3DHealthAI, S.L. ("iNuba"). If you link to a clinic or a professional, that professional decides about the clinical information they add themselves.
- **What information we handle.** Your account data, questionnaire answers, health variables (body measurements, biomarkers, wearable biometrics), the images and the analysis produced by the scan with the iNuba Hardware, and your subscription data.

- **What we use it for.** To provide you with the service, build your history and show you your progress (ordinary operation); to produce statistics using anonymised data that no longer identifies you, which you can object to; and, only if you authorise it through separate checkboxes, to train our technology with your images and to share anonymised datasets with third parties.
- **Artificial intelligence.** Your nutrition and training plans are generated by AI systems. They are guidance proposals, reviewable by your professional, and they never decide anything about you with legal effects.
- **What you control.** The uses involving images each have their own checkbox, revocable from Settings; you can object to the statistics based on anonymised data whenever you like. The service works exactly the same in every case.
- **Where your information is held.** In the European Union (France). Certain providers may involve transfers to the United States: section 8.
- **What you can require from us.** Access, rectification, erasure, objection, restriction, portability and withdrawal of consents, by writing to dataprotection@inuba.com.

1. Data Controller

3DHealthAI, S.L. ("iNuba"), Polígono Industrial Los Vientos, C/ Levante, 1, 46119 Náquera (Valencia), Spain, NIF B-40644445.

Data Protection Officer: dataprotection@inuba.com.

2. When this text applies and who decides what

Versions under a third-party brand (white label). This policy applies equally when you use the App under the brand of a Partner Entity: iNuba remains the Data Controller for the processing of your information in the App. If you access it that way, part of your data does not come from you but from the Partner Entity (sections 3.1 and 7), and we inform you of this in accordance with Article 14 GDPR.

Allocation of roles within the iNuba ecosystem. iNuba acts as **Data Controller** for the information you generate using the App, the iNuba Hardware and your devices. When you link to a professional or clinic through iNuba Clinic, it is that professional who acts as **Data Controller** for the clinical information they manually add about you (clinical record,

observations, protocols and the plans they assign to you), with iNuba acting as their **Data Processor**. Certain processing operations within the ecosystem - registration and linking, the activity history and the synchronisation between the App and the professional platform - are determined jointly; the essential terms of the agreement entered into between iNuba and your professional are available to you on request.

3. What information we process

3.1 Account and profile

Email address, password - held by our identity provider, Google Firebase, and never stored by iNuba -, language and device. If you register with Google or Apple: your email address and the basic profile data the provider passes on to us, including first name and surname, which we use to pre-fill your initial questionnaire. Profile photograph, which is optional.

If you access through a white label version, the Partner Entity passes on to us your identification data (name, email address, identity document and date of birth), your access status and, where it holds them, health profile data (ethnic origin, declared conditions, sex, height and weight), in order to register you and maintain your access.

3.2 Initial questionnaire and health profile

First name and surname, date of birth, sex, ethnic origin, country, height, weight, goal pursued, lifestyle, type and frequency of physical activity, and medical conditions. Ethnic origin and medical conditions are special category data: we process them on the basis of your explicit consent, in order to calibrate both the variables and the proposals you receive correctly.

3.3 Health variables recorded in the App

- Body and body composition measurements (weight, girths, fat and lean mass, and body water, among others).
- Biomarkers and blood test results: total cholesterol, HDL and LDL, triglycerides, vitamin D, ferritin, TSH, CRP, uric acid, creatinine, iron and haemoglobin.
- Clinical and laboratory variables: glycated haemoglobin, D-dimer, bone density, full spirometry, temperature, cardiovascular risk index and prothrombin time.
- Skin assessment: sun damage, elasticity, phototype, hydration, acne, pigmentation, porosity, keratinisation, redness and texture.

- Skinfolds: triceps, biceps, subscapular, suprailiac, supraspinal, abdominal, chest, front thigh and medial calf.
- Daily record of habits and wellbeing: mood, perceived stress, energy, appetite, hydration, rest (duration, time bands and quality) and steps.
- Information generated by the nutrition and training plans assigned to you, and by the automated protocols configured by your professional.

Every variable keeps a trace of its origin: entered by you, imported from the iNuba Hardware, received from a wearable, or added by your professional.

3.4 Wearables and health platforms on your device

Subject to your authorisation in the operating system:

- **Apple Health (read only):** rest, workouts, heart rate and resting heart rate, heart rate variability (HRV), glucose, oxygen saturation, blood pressure and steps. We write no data whatsoever to Apple Health.
- **Health Connect - Android (read only):** steps, rest, workouts, heart rate and resting heart rate, HRV, glucose, oxygen, blood pressure, distance and calories. Here too we write nothing.

Synchronisation may take place in the background even when the App is closed, through periodic operating system tasks. The transmission is authenticated with a technical key specific to your user account, which can be revoked. You can withdraw the permissions at any time from your device settings.

3.5 Scanning with iNuba Hardware

RGB images captured by three cameras, thermography, bioimpedance obtained from two scales, answers to the prior questionnaire (pregnancy, pacemaker and implants) - used at the very moment of the scan to determine whether the bioimpedance measurement should be taken - and the environmental variables of the session entered by your professional.

3.6 Questionnaires and protocols

Answers to the questionnaires sent to you by iNuba or your professional, their completion status and their history; and the record of the actions triggered by the automated protocols your professional may have configured (messages, measurement requests and reminders), with their date and their outcome.

3.7 Alerts

Record of the notices generated when a variable exceeds the margins set by your professional, stating the variable concerned, the value, the threshold and the time.

3.8 Subscription and billing

Subscription identifiers, amounts and payment status managed by the app stores, together with the tax details needed to issue an invoice where applicable. iNuba has no access to your card details.

3.9 Technical usage information

Device identifiers, App usage events for analytics purposes, error reports and consent records (date, IP address, device, language, version and digital fingerprint of the document accepted).

3.10 Demonstration accounts

There are "demo" accounts populated with synthetic data that does not correspond to real people, intended for clinics to evaluate the product. As they are not personal data, they fall outside the retention cycles.

4. Purposes and legal bases

Purpose	Legal basis
Providing you with the service: account, health monitor, scan and avatar, plans, questionnaires, protocols and alerts	Performance of the contract (Art. 6(1)(b) GDPR) and, for health data, your explicit consent (Art. 9(2)(a) GDPR)
Linking to your professional or clinic and their access to your information	Your explicit consent (Arts. 6(1)(a) and 9(2)(a) GDPR), given when you accept the linking invitation. In white label versions of occupational health services or healthcare entities, the disclosure of your scan results to the entity relies on your explicit consent given at registration, and the entity processes them under its own legal basis (Art. 9(2)(h) GDPR and health surveillance legislation, where applicable)
Generation of	Performance of the contract (Art. 6(1)(b) GDPR) and

Purpose	Legal basis
nutrition and training plans by means of artificial intelligence systems	explicit consent for health data (Art. 9(2)(a) GDPR). See section 5
Billing, payment collection and compliance with tax obligations	Legal obligation (Art. 6(1)(c) GDPR)
Operational and care-related communications	Performance of the contract (Art. 6(1)(b) GDPR)
Commercial communications	Your consent (Art. 6(1)(a) GDPR), revocable from Settings
Usage analytics and technical improvement (Firebase)	Legitimate interest in improving the service (Art. 6(1)(f) GDPR), with minimised data; on iOS, additionally subject to tracking permission (ATT)
Security, fraud prevention and evidencing of consents	Legitimate interest (Art. 6(1)(f) GDPR) and duty to demonstrate compliance (Art. 7(1) GDPR)
Aggregated statistics and improvement using anonymised data (variables, never images)	Legitimate interest and compatibility with statistical purposes (Arts. 6(1)(f), 5(1)(b) and 89 GDPR), with the right to object. See section 6.2
Training of our technology with images and associated research; sharing of anonymised individual-level datasets	Your specific consent, separate for each purpose (Arts. 6(1)(a) and 9(2)(a) GDPR, with the safeguards of Art. 89). See sections 6.3 and 6.4

5. Artificial intelligence

5.1. What it consists of. The nutrition and training plans you receive, as well as certain support functions of the automated protocols, are produced by artificial intelligence systems operated by iNuba. We inform you of this expressly in compliance with the transparency obligations of Regulation (EU) 2024/1689 on artificial intelligence and with Article 13 GDPR.

5.2. What information is used. To generate a proposal we use your profile data, your goals, your recorded health variables, the biometrics coming from wearables, the scan results and your questionnaire answers. Your body images and your thermographies are not used to generate plans.

5.3. No automated decisions with legal effects. These systems produce guidance recommendations. No decisions are taken based solely on automated processing that produce legal effects concerning you or similarly significantly affect you (Art. 22 GDPR). Where there is a linked professional, they can review, adjust, replace or discard any proposal before assigning it to you, and their professional judgement remains intact.

5.4. Limitations. The output of an artificial intelligence system may be inaccurate. We apply reasonable validation and quality control measures, but this does not allow us to guarantee absolute accuracy. Consult your doctor or healthcare professional before incorporating any proposal into your routine, and especially so where there are medical conditions, pregnancy, breastfeeding, allergies, intolerances or ongoing medication.

5.5. What you can ask us for. You can request additional information at dataprotection@inuba.com about the general logic applied and, through your linked professional, human review of a specific proposal.

5.6. Model training. The use of your information to train and improve these systems is governed by sections 6.2 and 6.3, and it never takes place with identifiable images without your express and separate authorisation.

6. Your images and your data: ordinary operation and the decisions that are yours

6.1 Provision of the service, history and progress (ordinary operation)

Your scan images, three-dimensional avatars, thermographies and variables are stored and used to produce your results, your history and your progress comparison for as long as you keep the account. This includes the technical

operations that are essential to run, maintain, ensure the quality of and technically improve the service you receive - error correction, calibration of results and security -, which form part of the service itself. Legal basis: performance of the contract and your explicit health consent given at registration (Arts. 6(1)(b) and 9(2)(a) GDPR). This information is only deleted if you exercise your right to erasure or delete your account, in which case the legal blocking periods in section 9 apply.

6.2 Aggregated statistics and improvement using anonymised data (ordinary operation, with the right to object)

We produce statistics, analyses and studies using irreversibly anonymised and aggregated data - health variables, never images - for the dual purpose of improving our services and of compiling reports and statistical datasets for the health sector, which may be shared with or sold to third parties. Such datasets no longer allow you to be identified and cease to be personal data (Recital 26 GDPR). The prior anonymisation step relies on our legitimate interest and on its compatibility with statistical purposes, with the safeguards of Article 89 (Arts. 6(1)(f) and 5(1)(b) GDPR), following an impact assessment and applying a minimum aggregation threshold.

You can object whenever you wish by writing to dataprotection@inuba.com: your information will stop being included in the datasets generated from that moment on, and those already anonymised can neither be reversed nor attributed to you. The information of minors is excluded.

6.3 Training and improvement of our technology with your images (requires authorisation)

This processing is not yet operational. Your body images and thermographies may contribute to training and improving our technology - the three-dimensional avatar and new health features - as well as to the associated scientific research, with the safeguards of Article 89 GDPR. Since images cannot be fully anonymised, this use will only be activated if you authorise it through a specific and separate checkbox (Arts. 6(1)(a) and 9(2)(a) GDPR), which we will ask you for at the appropriate time - for example, after your first scan - and which you will be able to manage from Settings → My consents.

What happens if you withdraw your authorisation. Your images are not deleted: they remain stored in order to provide you with the service under section 6.1. They simply stop being used in training and are excluded from

subsequent model improvement cycles. Models already trained do not contain identifiable personal data and do not allow immediate individual extraction, a limitation we disclose to you transparently; those models may be licensed to third parties in the health sector. Your images are only deleted if you exercise your right to erasure. Retention for this purpose: for as long as your authorisation subsists and, in any event, within the periods in section 9. Before activating this processing, the impact assessment required by Article 35 GDPR will be completed.

6.4 Sharing anonymised individual-level datasets with third parties (requires authorisation)

Beyond the aggregated statistics in section 6.2, we may compile irreversibly anonymised individual-level datasets - person-level records that no longer allow you to be identified - and share them with third parties in the health sector (laboratories, insurers, academic institutions or medical device manufacturers) for research, statistical or health product and service development purposes. **This processing is not operational either:** its activation will be preceded by the corresponding impact assessment and by technical anonymisation controls with a minimum aggregation threshold, and you will be notified of it. The sharing will only be activated if you authorise it through a specific and separate checkbox, revocable whenever you wish from Settings → My consents or by writing to dataprotection@inuba.com. The information of minors and the data coming from third-party health platforms and wearables (Apple Health, Health Connect and any integrations added in future, such as Garmin or Whoop) are excluded, as the terms of those platforms prohibit sharing them. No image is shared with third parties.

None of the uses in this section conditions the ordinary operation of the App: the service is identical whether or not you tick the boxes and whether or not you exercise your right to object.

7. Who else accesses your information

- **Linked professional or clinic.** Once the linking invitation is accepted, they access the whole of your clinical information; there are no forms of linking with reduced access. They also add their own information about you, for which they are the Data Controller. You can unlink whenever you wish from the App, with the effect set out in the General Conditions of Use.

- **Company (Corporate).** If you link to one, it knows your membership (organisation, site and department) and your answers to the questionnaires it sends you itself, stored in association with your user account. Check the specific information for each questionnaire before answering.
- **Partner Entity (white label).** If you access under its brand, that entity knows that you are its customer and the status of your access to the App, which it administers itself. Where the Partner Entity is also your occupational health service or your healthcare entity and the scan is performed within its activity, we disclose the result to it: your body measurements, your body composition, your temperatures and your thermographic images. Outside that situation it receives no health information or images. It acts as an independent Data Controller, both for its commercial relationship with you and for the information we pass on to it.
- **Processors and providers.** Amazon Web Services (hosting and storage, Paris region, EU) and OVHcloud (France); Apple, Google and RevenueCat (management of the Premium subscription; we disclose to RevenueCat, together with your identifier, your email address, your name and your date of birth); Google Firebase (identity and authentication provider, and usage and error analytics: the names of certain events reflect the category of the data recorded - glucose, for example - without personal values or identifiers, and your identifier travels obfuscated in error reports); AWS SES (transactional email); ActiveCampaign (United States; if you access through a corporate code, it receives your email address, your name and your organisation for the management of our communications).
- **Artificial intelligence providers.** The systems used to generate your plans run on iNuba infrastructure or on third-party services engaged as Data Processors, subject to a contractual undertaking not to use your information to train their own models and to delete it once the processing is complete. The up-to-date list of these providers, with their location and their safeguards, is published at inuba.com/legal.
- **Public authorities, courts and law enforcement agencies,** where there is a legal obligation.

8. Data location and international transfers

The servers and backups are located in the European Union (France). Certain providers - Google and Firebase, RevenueCat, ActiveCampaign and, where

applicable, the artificial intelligence providers - may involve transfers to the United States, relying on the EU-US Data Privacy Framework or on standard contractual clauses. You can request additional information from the Data Protection Officer.

9. How long we keep your information

- **Active account:** for as long as you keep it.
- **After deleting the account:** immediate logical deletion; the data is blocked and health data linked to care processes is kept for five (5) years (Ley 41/2002), the user's tax data for four (4) years and the applicable commercial documentation for six (6) years. Once those periods have elapsed, it is irreversibly anonymised or deleted.
- **Images, three-dimensional models and thermographies:** they are kept for the periods set out above and, on their expiry, are irreversibly deleted or anonymised. You can request the deletion of your images whenever you wish at dataprotection@inuba.com. If you give the consent in section 6.3, the specific period for that purpose is five (5) years.
- **Consent records:** these are kept as evidence of compliance with Article 7(1) GDPR for as long as the account remains active and for the periods in this section after termination.
- **Records of questionnaires, protocols and alerts:** for the duration of the link with the clinic and the applicable healthcare retention periods.

10. What you can require from us

You can exercise the rights of access, rectification, erasure, objection, restriction and portability, and withdraw any consent, at dataprotection@inuba.com or from the App itself:

- **My consents (Settings):** full history and withdrawal by type.
- **Erasure:** Settings → Account → Delete account (see clause 14 of the General Conditions of Use).
- **Access:** from the App you can consult your information, your history of completed questionnaires and your consents; to obtain a full copy, request it from the Data Protection Officer.
- **Rectification:** edit your profile or request it from the Data Protection Officer.

Response time: one month (Art. 12(3) GDPR). You may lodge a complaint with the Spanish Data Protection Agency (AEPD) (aepd.es).

11. Security measures

We apply encryption in transit (TLS) for communications with the App, access control through authenticated identity and service keys, logical isolation per customer, verification of the cryptographic signature of the notifications from our payment provider, data aggregation in analytics processes, and daily encrypted backups of our databases, hosted on separate infrastructure within the European Union. No system is infallible; we will notify breaches in accordance with Articles 33 and 34 GDPR.

12. Minimum age

The App requires you to be sixteen (16) years old. We do not knowingly process information about children below that age; if we become aware of an account in that situation, we will delete it. The information of minors is excluded from the uses described in sections 6.2 and 6.4.

13. Updates to this text

We will publish successive versions stating their effective date and digital fingerprint, and we will obtain re-acceptance where the significance of the change requires it. The version history remains available at inuba.com/legal.