

Table of Contents

PRIVACY POLICY — iNuba App.....1

At a glance.....1

1. Data Controller.....2

2. Data we process.....2

3. Purposes and legal bases.....4

4. How we use your images and data: what works by default and what you control.....5

5. Recipients and processors.....7

6. International transfers.....8

7. Retention periods.....8

8. Your rights.....9

9. Security.....9

10. Minors.....10

11. Changes to this policy.....10

PRIVACY POLICY — iNuba App

Version 2.1 · In force from: 20 July 2026

At a glance

- **Who processes your data:** 3DHealthAI, S.L. (iNuba). If you link to a professional or clinic, they are the Data Controller of the clinical data they enter.
- **What we process:** account data, questionnaires, health data (body metrics, biomarkers, medication, wearables), body images from the 3D scans, your purchases and your communications with your professional.
- **What for:** to provide you with the service, your history and your progress (by default); aggregated statistics using anonymised data that no longer identifies you, with a right to object; and, only if you

authorise it through separate checkboxes, the training of our technology with your images and the transfer to third parties of anonymised data sets.

- **You decide:** the uses involving images have their own checkbox, revocable in Settings; you can object at any time to the statistics using anonymised data. The main service works exactly the same in all cases.
 - **Where your data is:** in the European Union (France). Some providers may involve transfers to the United States: see section 6.
 - **Your rights:** 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.

This policy also applies when you use the App under the brand of a Partner Entity (white label version): iNuba remains the Data Controller of your data in the App. When you access through this route, part of your data is not provided by you but by the Partner Entity (see sections 2.1 and 5); we inform you of this in accordance with Article 14 GDPR.

Dual role in the iNuba ecosystem: iNuba is the **Data Controller** of the data you generate by using the App, the iNubaBox/Totem booth and your devices. When you link to a professional or clinic through iNuba Clinic, that professional is the **Data Controller** of the clinical data they enter manually about you (notes, clinical record, reports), with iNuba acting as **Data Processor** on their behalf. Certain processing operations within the ecosystem (linking, activity history, chat) are carried out jointly; the essential aspects of the arrangement between iNuba and your professional are available to you upon request.

2. Data we process

2.1 Account and profile

Email address, password (held by our identity provider, Google Firebase; iNuba does not store it), language, device. If you register with Google or Apple, your email address and the basic profile data provided to us by that provider (including your first name and surname, which we use to pre-fill your initial questionnaire). Optional profile photo. If you access through a white label version, the Partner Entity communicates to us your identification data (name, email address, identity document and date of birth), your access status and, where it holds them, data from your health profile (ethnic origin, declared conditions, sex, height and weight), in order to register you and maintain your access.

2.2 Initial questionnaire and health profile

First name and surname, date of birth, sex, **ethnic origin**, country, height, weight, goal, lifestyle, type and frequency of activity, and medical conditions. Ethnic origin and medical conditions are special category data: we process them with your explicit consent in order to calibrate metrics and plans correctly.

2.3 Health data generated in the App

- Body and body composition metrics (weight, girths, fat/lean mass, water, etc.).
- Biomarkers and blood tests: total/HDL/LDL cholesterol, triglycerides, vitamin D, ferritin, TSH, CRP, uric acid, creatinine, iron, haemoglobin.
- Clinical and laboratory metrics: glycated haemoglobin, D-dimer, bone density, full spirometry, temperature, cardiovascular risk index, prothrombin time.
- Skin analysis: sun damage, elasticity, phototype, hydration, acne, pigmentation, porosity, keratinisation, redness, texture.
- Skinfolds (triceps, biceps, subscapular, suprailiac, supraspinal, abdominal, pectoral, anterior thigh and medial calf).
- Daily wellbeing log: mood, subjective stress, energy, appetite, hydration, sleep (duration, hours, quality) and steps.
- Medication and treatments: name, category, dose, dosage by time slot, frequency, dates, remarks and **adherence** (doses taken, missed, on time), and downloadable test reports.

- Food diary: foods consumed, custom products with their full nutritional profile and product photograph, favourites by barcode.
- Data generated by your nutrition, fitness and mind plans.

The source of health metrics is recorded (entered by you, imported from the booth, from a wearable or from your professional).

2.4 Wearables and health platforms

With your authorisation in the operating system: Apple Health (read): sleep, workouts, heart rate and resting heart rate, variability (HRV), glucose, blood oxygen, blood pressure and steps. We do not write any data to Apple Health. Health Connect – Android (read): steps, sleep, workouts, heart rate and resting heart rate, HRV, glucose, oxygen, blood pressure, distance and calories. No writing. Background synchronisation: the App may collect this data even when closed, by means of periodic system tasks and notifications from the operating system itself. Transmission is authenticated with a technical key specific to your user, which is revocable. You can revoke the access permissions to this data at any time from your device settings.

2.5 iNubaBox / Totem scan

RGB images (three cameras), thermography, bioimpedance (two scales), answers to the prior questionnaire (pregnancy, pacemaker, prostheses), which are used at the time of the scan to decide whether the bioimpedance is performed **or** not, and environmental variables of the session entered by your professional.

2.6 Appointments, classes and informed consents

Bookings, prior requirements demanded by your professional (answers to questionnaires, measurements, **photographs** you upload and **digitised handwritten signature** of consent documents), attendance, absences and applicable penalties, and waiting lists (name and telephone number).

2.7 Chat and communications

Messages with your clinic/professional and attached files (which may contain health data), labelled according to the sender (you, a professional or automated messages from the clinic). Operational, care-related (medication reminders, clinical alerts) and, with your consent, commercial push notifications.

2.8 Purchases and billing

Orders, amounts, payment method (handled by Stripe; iNuba does not see your card), email address communicated to Stripe for the charge and the receipt, and tax data (NIF, postcode/tax address) where required for invoicing. Purchase history and invoices.

2.9 Technical use

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

2.10 Demonstration accounts

There are "demo" accounts with **synthetic** data (they do not correspond to real people) so that clinics can try out the product; they are excluded from the retention cycles for personal data because they are not personal data.

3. Purposes and legal bases

Purpose	Legal basis
Providing you with the service (account, plans, monitor, avatar, chat, appointments, shop)	Performance of the contract (Art. 6(1)(b) GDPR) and, for health data, your explicit consent (Art. 9(2)(a))
Linking with your professional/clinic and their access to your data	Your explicit consent (Arts. 6(1)(a) and 9(2)(a)), given when you accept the linking invitation; in the white label versions of occupational risk prevention services or healthcare entities, the disclosure of the result of your scans to the entity is based on your explicit consent given at registration, with the entity processing it under its own legal basis (Art. 9(2)(h) GDPR and health surveillance legislation, where applicable)
Billing, payments and tax obligations	Legal obligation (Art. 6(1)(c))
Operational and care-related communications	Performance of the contract (Art. 6(1)(b))

Purpose	Legal basis
Commercial communications (push/promotions)	Your consent (Art. 6(1)(a)), revocable in Settings
Usage analytics and technical improvement (Firebase)	Legitimate interest in improving the service (Art. 6(1)(f)), with minimised data; on iOS additionally subject to tracking permission (ATT)
Security, fraud prevention and consent auditing	Legitimate interest (Art. 6(1)(f)) and the obligation to demonstrate compliance (Art. 7(1))
Aggregated statistics and improvement using anonymised data (metrics, never images)	Legitimate interest and compatibility with statistical purposes (Arts. 6(1)(f), 5(1)(b) and 89), with a right to object . See section 4.2
Training of the technology with images and associated research; transfer of anonymised individual-level data	Your specific and separate consent for each purpose (Arts. 6(1)(a) and 9(2)(a), with the safeguards of Art. 89). See sections 4.3 and 4.4

We do not take automated decisions producing legal effects concerning you (Art. 22 GDPR): the plans are indicative recommendations—not a medical prescription or healthcare advice—and, where a professional is linked, they are supervised by them. Consult your doctor or a trusted professional before making significant changes.

4. How we use your images and data: what works by default and what you control

4.1 Provision of the service, history and progress (by default: this is the service)

Your scan images, 3D avatars, thermographies and metrics are stored and used to generate your results, your history and your comparison of progress over time, for as long as you keep your account. This use includes the technical operations necessary to run, maintain, ensure the quality of and technically improve the service you receive (error correction, calibration of results, security), which form part of the provision of the service. Legal basis: performance of the contract and your explicit health-data consent given at

registration (Arts. 6(1)(b) and 9(2)(a) GDPR). **These images and data are only deleted if you exercise your right to erasure or delete your account** (in which case the legal blocking periods of section 7 apply).

4.2 Aggregated statistics and improvement using anonymised data (by default, with a right to object)

We produce statistics, analyses and studies using data that is **irreversibly anonymised and aggregated** —health metrics and variables; **never images** — in order to improve our services and to produce reports and statistical data sets for the health sector which we may share with, or commercialise to, third parties. These data sets no longer allow you to be identified and cease to be personal data (Recital 26 GDPR). The prior anonymisation step is based on our legitimate interest and its compatibility with statistical purposes, with the safeguards of Art. 89 (Arts. 6(1)(f) and 5(1)(b) GDPR), following the corresponding impact assessment and with a minimum aggregation threshold.

You can object at any time by writing to dataprotection@inuba.com: your data will cease to be incorporated into new data sets generated from that moment on (those already anonymised cannot be reversed or attributed to you). Data relating to minors is excluded.

4.3 Training and improvement of our technology using your images (requires your authorisation)

This processing is not operational yet. Your body images and thermographies may help us to train and improve our technology: the 3D avatar and new health features, as well as the associated scientific research (with the safeguards of Art. 89). Since images cannot be fully anonymised, this use is only activated **if you authorise it by means of a specific and separate checkbox** (Arts. 6(1)(a) and 9(2)(a) GDPR), which we will ask you for at the appropriate moment (for example, after your first scan) and which you **will be able to** manage in Settings → My consents.

Important — what happens if you withdraw your authorisation: your images are not deleted; they remain stored in order to provide you with the service in accordance with section 4.1. They simply cease to be used for 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 which we disclose to you honestly; 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 you maintain your authorisation and, in any event, no longer than the retention periods of section 7. Before activating this processing, the impact assessment required by Art. 35 GDPR will be completed.

4.4 Transfer of anonymised individual-level data sets to third parties (requires your authorisation)

In addition to the aggregated statistics of section 4.2, we may produce data sets that are **individual-level and irreversibly anonymised** (person-level records that no longer allow you to be identified) and transfer them to 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 yet**: when it is activated, it will first be subject to an impact assessment and to technical anonymisation controls with a minimum aggregation threshold, and we will notify you. This transfer will only be activated if you authorise it by means of a specific and separate checkbox, which you may revoke at any time in Settings → My consents or by writing to dataprotection@inuba.com. Data relating to minors is excluded, as is data originating from third-party health platforms and wearables (Apple Health, Health Connect and any other integrations that may be added, such as Garmin or Whoop), whose transfer is prohibited by the terms of those platforms. No image is transferred to third parties.

None of the uses in this section affects the normal operation of the App: the service is the same whether or not you tick the checkboxes and whether or not you exercise your right to object.

5. Recipients and processors

- **Linked Professional/clinic**: they access your set of clinical data only if your relationship is that of "customer"; as a "contact" they do not access clinical data or private chat. They also enter their own data about you, of which they are the Data Controller.
- **Company (Corporate)**: if you link, it knows your affiliation (company, site, department) and your answers to its corporate surveys, which are stored linked to your user account. Check the specific information for each survey before answering.

- **Partner Entity (white label):** if you access under its brand, that entity knows that you are its customer and your access status in the App, which it manages itself. Where the Partner Entity is also your occupational risk prevention service or your healthcare entity and the scan is carried out within the scope of its activity, we communicate the result of your scan to it: your body metrics, your body composition, your temperatures and your thermographic images. Outside that scenario, it does not receive your health data or your images. It is an independent Data Controller both of its commercial relationship with you and of the data we communicate to it.
- **Processors and providers:** Amazon Web Services (hosting and storage, Paris region, EU) and OVHcloud (France); Stripe (payments; receives your email address and, where applicable, your tax location for tax calculation); Apple/Google/RevenueCat (Premium subscription; to RevenueCat we communicate, in addition to your identifier, your email address, your name and your date of birth); Google Firebase (identity and authentication provider; usage and error analytics; the names of some events reflect the category of the data recorded —e.g. glucose—, without personal values or identifiers; in error reports your identifier is transmitted in obfuscated form); AWS SES (transactional email); ActiveCampaign (United States; if you access by means of a corporate code, it receives your email address, your name and your company in order to manage our communications);
- **mediQuo** (telemedicine): independent Data Controller. When you activate it we communicate to it: user code, first name and surname, sex, plan, date of birth, email, telephone number and language. We do not communicate your clinical history to it. The content of your consultations resides with mediQuo.
- **OpenFoodFacts:** the barcode lookup does not communicate any personal data (only the code or text searched for).
- **Google (Calendar/Meet):** if your clinic connects its Google account, the meeting for your online appointment/class is created in the clinic's calendar; the title of the service and the time are communicated to Google. At present neither your name nor your email address is communicated.
- Public authorities, courts and law enforcement bodies where there is a legal obligation.

6. International transfers

The servers and backups are located in the **European Union** (France). Some providers (Google/Firebase, Stripe, RevenueCat, ActiveCampaign) may involve transfers to the United States; these are based on the EU-US Data Privacy Framework and/or standard contractual clauses. You may request additional information from the DPO.

7. Retention periods

- **Active account:** for as long as you keep it.
- **Upon deletion of the account:** immediate logical deletion; the data are blocked and retained for **5 years** in the case of health data linked to healthcare processes (Ley 41/2002), **4 years** in the case of user tax data and **6 years** in the case of the applicable commercial documentation; thereafter it is irreversibly anonymised or erased.
- **Images and 3D models/thermographies:** they are retained for the periods indicated above; upon expiry they are deleted or irreversibly anonymised. You may request the deletion of your images at any time at dataprotection@inuba.com. If you consent to the research described in section 4.3, the specific period for that purpose is 5 years.
- **Consent records:** they are retained as evidence of compliance with Art. 7(1) GDPR for as long as your account is active and for the retention periods set out in this section following termination.
- **Chat and attachments:** for the duration of the link and the applicable healthcare retention periods. Upon expiry, the content of the messages and their attached files is anonymised or deleted.

8. Your rights

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

- **My consents** (Settings): full history and withdrawal by type.
- **Erasure:** Settings → Account → Delete account (see T&C, clause 12).
- **Access:** in the App you can consult your data, your history of completed clinical questionnaires and your consents; for a full copy, request it from the DPO.
- **Rectification:** edit your profile or request it from the DPO.

Response time: one month (Art. 12(3)). Complaints: Spanish Data Protection Agency (AEPD) (aepd.es).

9. Security

We apply encryption in transit (TLS) for communications with the App, access control based on authenticated identity and service keys, logical isolation per customer, verification of the cryptographic signature of our payment provider's webhook, aggregation of data in analysis processes and daily encrypted backups of our databases, stored on separate infrastructure within the European Union. No system is infallible; we will notify personal data breaches in accordance with Arts. 33-34 GDPR.

10. Minors

The App requires users to be at least **16 years of age**. We do not knowingly process data of children under 16; if we become aware of such an account, we will delete it. Data relating to minors is excluded from the uses described in sections 4.2 and 4.4.

11. Changes to this policy

We will publish new versions with their date of entry into force and digital fingerprint, and we will ask for your re-acceptance where the change so requires. The version history is available at inuba.com/legal.
