

Table of Contents

iNuba CLINIC PRIVACY POLICY (PROFESSIONALS).....	1
Purpose and scope of this document.....	1
1. Data Controller.....	1
2. Information we process.....	2
3. Purposes and legal bases.....	2
4. Who else accesses your information.....	3
5. Data location and international transfers.....	4
6. How long we keep your information.....	4
7. Your rights.....	5
8. Security measures.....	5
9. Cookies.....	5
10. Updates to this text.....	5

iNuba CLINIC PRIVACY POLICY (PROFESSIONALS)

Version 2.0 · Effective date: 7 August 2026

Purpose and scope of this document

This text is addressed to the professionals, Account Holders and staff of Customer entities ("you") and describes how we process **your** personal information when you use iNuba Clinic.

It does not cover the processing of the information of your **End Users** - the users of the iNuba app linked to your clinic - which is governed by the Data Processing Agreement (Annex 1 to the iNuba Clinic General Conditions) and, as regards the data for which iNuba is the Data Controller, by the iNuba App Privacy Policy.

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. Information we process

Identification and account. Name, email address, encrypted password, telephone number, business sector, working arrangement and the other details collected during onboarding - client volume, teamwork, website, services of interest and how you heard about us; the profile assigned to you and the entity you belong to; profile photograph, which is optional. If you sign in with Google: email address and name.

Tax and billing information of the entity. Company name, NIF or CIF, address, billing email address, CNAE code and currency, together with the subscription identifiers. Card details are processed by Stripe, and iNuba has no access to them.

Use of the Platform. Access and seat logs, account activity - changes of plan and seats, and lifecycle events -, audited access to blocked records, and consents and acceptances of the legal texts, recording the date, IP address, device, version and digital fingerprint of the document.

Communications. Transactional emails - verification, billing, payment incidents, invitations, pending-task notices, password reset and account closure - and support requests. If you use the WhatsApp help button, available on the Pro and Platinum plans, the conversation takes place on WhatsApp (Meta) and is associated with your number.

Information received from third parties. Where your registration comes from an authorised distributor, the distributor provides us with the name of the clinic, and the email address and telephone number of the Account Holder and, where applicable, the CIF.

Web analytics. On the public pages we use Google Analytics 4 only if you accept cookies, with consent denied by default. In the private area we operate no third-party analytics. Certain conversion events are also reported server-side, relying on the identifier captured with your cookie consent.

3. Purposes and legal bases

Purpose	Legal basis
Registration, authentication and provision of the Platform, including, where applicable,	Performance of the contract (Art. 6(1)(b) GDPR)

Purpose	Legal basis
management of White Label Mode (API credentials, branding and billing of the mode)	
Subscription billing and compliance with tax obligations	Legal obligation (Art. 6(1)(c) GDPR)
Management of payment incidents: staged notices, suspension and closure	Performance of the contract and legitimate interest (Arts. 6(1)(b) and 6(1)(f) GDPR)
Operational service communications	Performance of the contract (Art. 6(1)(b) GDPR)
B2B commercial communications about iNuba and management of the trial and subscription cycle through our marketing tool	Legitimate interest in commercial communications between professionals (Art. 6(1)(f) GDPR), with the right to object in every message and at dataprotection@inuba.com
Analytics on the public pages	Consent given in the cookie banner
Security, auditing and evidencing of consents	Legitimate interest (Art. 6(1)(f) GDPR) and duty to demonstrate compliance (Art. 7(1) GDPR)
Relationship with distributors: attribution of the registration and subscription status	Legitimate interest and performance of the contract

4. Who else accesses your information

- **Stripe:** payment processing, billing and tax calculation.

- **Amazon Web Services** (European Union, Paris region) and **OVHcloud** (France): hosting. **Amazon SES**: transactional email.
- **ActiveCampaign** (United States): marketing tool; it receives your email address, your name and the status of your trial or subscription for the management of our commercial communications. It receives no information whatsoever about End Users. The transfer relies on the EU-US Data Privacy Framework or on standard contractual clauses, under a data processing agreement.
- **Calendly**: scheduling of demonstrations and commercial meetings; if you request a meeting from the Platform or from our website, it receives your name, your email address and the booking details.
- **Google**: Analytics 4, only where you have given your cookie consent, with a possible transfer to the United States under the safeguards cited above; and identity provider, where you sign in with Google.
- **Meta (WhatsApp)**: only if you use the help button; iNuba does not store that conversation.
- **Authorised distributor**: where your registration comes from a distributor, it receives the activation status and the subscription amounts of the clinic, with no End User data whatsoever.
- **Public authorities**, where there is a legal obligation.

5. Data location and international transfers

Hosting and backups are located in the European Union (France). Transfers to the United States arising from ActiveCampaign, Calendly, Google and Meta rely on the EU-US Data Privacy Framework or on standard contractual clauses. Further information: dataprotection@inuba.com.

6. How long we keep your information

- **Active account**: for as long as the relationship subsists.
- **After account closure**: four (4) years for the professional's information and six (6) years for the Account Holder's, in view of commercial and tax obligations; once those periods have elapsed, irreversible anonymisation.
- **Consent and acceptance records**: these are kept as evidence of compliance with Article 7(1) GDPR for the duration of the relationship and for the periods set out above following closure.
- **Payment incident cycle**: a suspended account retains its information and may be reactivated by payment until day 67; once closure has

occurred, the periods set out above apply, with the possibility of restoration during the retention period by requesting it from iNuba and subject to the re-acceptance of the texts in force.

7. Your rights

You may exercise the rights of access, rectification, erasure, objection - including objection to B2B commercial communications -, restriction and portability, and withdraw the consents given, by writing to dataprotection@inuba.com. The Platform itself provides you with the consents screen and the history of acceptances.

Supervisory authority: Spanish Data Protection Agency (AEPD) (aepd.es).

8. Security measures

Encryption in transit (TLS) for communications with the Platform, profile-based access control, mandatory email verification, tamper-evident record of acceptances, auditing of access to blocked records, daily backups on a separate server within the European Union, and logical isolation per company.

9. Cookies

The public pages display a banner with genuine accept and reject options; analytics remain disabled by default. The details are published at inuba.com/politica-de-cookies.

10. Updates to this text

We will publish successive versions stating their date and digital fingerprint; where appropriate, re-acceptance will be obtained through the Platform's mandatory acceptance screen.