

Privacy Policy — InASnap

Last updated: 18th April 2026 Version: 1.0

This English version is a courtesy translation. In case of any discrepancy, the Italian version prevails pursuant to Article 12 of Regulation (EU) 2016/679 («GDPR»).

1. Data Controller

The Data Controller is:

Andrea Longo Sole trader / Self-employed professional under Italian law Italian VAT number: **05700640286** Italian tax code: **LNGNDR96T24G224N** Registered address: **Via Andrea Cesalpino 2/A, 35136 Padova, Italia** E-mail: privacy@inasnap.app

(hereinafter also «InASnap» or «Controller»)

A Data Protection Officer (DPO) has not been designated as the conditions of Article 37 GDPR do not apply.

2. Scope

This Privacy Policy describes how InASnap processes personal data of users interacting with the following services (collectively, the «**Services**»):

- **inasnap.app** and subdomains — corporate website and waitlist landing page;
- **admin.inasnap.app** — SaaS application reserved for restaurant operators who manage their digital menus («Business Customers» or «Tenants»);
- **menu.inasnap.app** — public pages displaying the restaurant menu to end-customers who scan the QR code («End-Users»).

The Policy is provided pursuant to Articles 13 and 14 GDPR, Italian Legislative Decree 196/2003 as amended by Legislative Decree 101/2018 («Italian Privacy Code»), and the Guidelines of the Italian Data Protection Authority of 10 June 2021 on cookies and other tracking tools.

3. Roles

3.1 InASnap as **Data Controller** (Art. 4(7) GDPR)

InASnap acts as Controller with respect to:

- visitors of **inasnap.app** and waitlist leads;
- Business Customers registered on **admin.inasnap.app** (account, billing, service communications);
- navigation and aggregated analytics data relating to its own applications.

3.2 InASnap as **Data Processor** (Art. 28 GDPR)

For personal data of restaurant end-customers (e.g., visit identifiers generated on the public menu pages and any features that collect data entered by visitors), the Data Controller is the Business Customer that published the menu. InASnap acts as Data Processor and performs the processing on the documented instructions set out in the Terms and Conditions and in the DPA made available to Business Customers in the reserved area.

4. Categories of data, purposes and legal bases

4.1 Landing page visitors and waitlist (inasnap.app)

Data	Purpose	Legal basis
E-mail, preferred language	Waitlist subscription, launch communications	Consent (Art. 6(1)(a) GDPR)
Technical navigation data (IP, user-agent, timestamp)	Security, abuse prevention, site operation	Legitimate interest (Art. 6(1)(f) GDPR)
Google Analytics events (e.g., <code>join_waitlist</code>)	Measurement of landing page effectiveness	Consent (Art. 6(1)(a) GDPR) via cookie banner

4.2 Business Customers on admin.inasnap.app

Data	Purpose	Legal basis
E-mail, password (hash), name, surname, phone, avatar, language	Registration, authentication, account management	Performance of contract (Art. 6(1)(b) GDPR)
Google OAuth data (e-mail, name, Google ID)	Federated authentication as alternative to username/password	Performance of contract (Art. 6(1)(b) GDPR); involves transfer to Google LLC, USA
Business data of the restaurant (trading name, shop name, address, timezone, logo, description)	Menu publication service	Performance of contract (Art. 6(1)(b) GDPR)
User-generated content (menus, categories, dishes, prices, allergens, translations)	Storage, indexing, publication	Performance of contract (Art. 6(1)(b) GDPR)
Billing and payment data (name, billing address, Stripe customer ID, subscription ID, last 4 digits of card, plan, status)	Payment and invoicing for PRO / Onboarding plans	Performance of contract (Art. 6(1)(b) GDPR); legal obligation for tax/accounting (Art. 6(1)(c) GDPR)
Product usage logs (Mixpanel events): login, signup, feature usage, errors	Product improvement, troubleshooting	Legitimate interest (Art. 6(1)(f) GDPR) — right to object at any time
Menu texts submitted to the Claude model (Anthropic)	Automatic menu translation («AI Translation»)	Performance of contract (Art. 6(1)(b) GDPR) — feature activated on user request
Consent flags (Privacy Policy, Terms, optional newsletter)	Evidence of consent (Art. 7(1) GDPR)	Legal obligation of accountability (Arts. 5(2) and 24 GDPR)
Transactional e-mails (signup confirmation, invoices, expiry notices, security)	Fulfilment of contract	Performance of contract (Art. 6(1)(b) GDPR)

4.3 End-Users of the public menu (menu.inasnap.app)

For data collected on public menu pages, the Data Controller is the Business Customer that published the menu; InASnap acts as Processor under Article 28 GDPR. The Business Customer determines the applicable legal basis in its own privacy notice.

Data	Purpose	Legal basis (typical)
Session identifier (<i>ias_session_id</i> , UUID, sessionStorage) and visitor identifier (<i>ias_visitor_id</i> , UUID, localStorage)	Statistical measurement of menu visits, unique visitor distinction	Legitimate interest (Art. 6(1)(f) GDPR) if set up as first-party analytics equivalent to technical cookies, otherwise Consent (Art. 6(1)(a) GDPR + Art. 122 Italian Privacy Code)
Device type (MOBILE/TABLET/DESKTOP), user-agent, browser language	Usage statistics, rendering adaptation	Legitimate interest
UTM parameters (utm_source, utm_medium, utm_campaign), HTTP referrer	Measurement of access channels (QR codes, shared links)	Legitimate interest
Interaction events: PAGE_VIEW, MENU_VIEW, ITEM_CLICK	Statistics of dishes and categories viewed	Legitimate interest
IP address (in truncated/aggregated form at server level)	Security and abuse prevention	Legitimate interest (Art. 6(1)(f) GDPR)

The *ias_session_id* and *ias_visitor_id* identifiers are randomly generated client-side (UUID v4) and **contain no directly identifying data** (no name, e-mail, MAC address). They nonetheless qualify as «online identifiers» under GDPR recital 30 and are therefore personal data.

5. Source of the data

Data are collected (i) directly from the data subject through sign-up forms, profile fields, waitlist forms, Stripe checkout flows, and public menu interactions; (ii) from Google where the user chooses to log in with Google OAuth; (iii) from the user's browser for connection data (IP, user-agent, URL parameters); (iv) from the Business Customer where the latter uploads data relating to third parties. InASnap cannot verify the personal nature of such third-party data and places any notice obligation on the Business Customer acting as Controller.

6. Mandatory and optional data

Providing data for the purposes in sections 4.1 (waitlist) and 4.2 (registration, account management, payment, mandatory consents) is **mandatory**; refusal prevents activation of the Services. Providing data for product analytics (Mixpanel) and marketing is **optional** and refusal does not affect access to the Services.

7. Recipients and external Processors

The following sub-processors/Data Processors under Article 28 GDPR are used:

Provider	Location	Role	Data	Safeguards
Supabase Inc.	USA (EU data center — AWS eu-north-1, Stockholm, Sweden)	Authentication, database, storage, realtime	Credentials, profile, menu data, analytics events	DPA under Art. 28 GDPR; processing on EU servers; SCCs for any access from the US entity (Module 2)
Google LLC	USA (Google Ireland Ltd. for EEA)	(a) OAuth authentication; (b) Google Analytics 4 on landing page	Google profile data, navigation events	Certified under EU-US Data Privacy Framework; SCCs as

Provider	Location	Role	Data	Safeguards
				additional safeguard
Stripe Inc.	USA (Stripe Payments Europe Ltd. for EEA, Dublin, Ireland)	Payments, invoicing, subscription management	Billing data, Stripe customer IDs, last 4 digits (no full PAN or CVV stored by InASnap)	Stripe Payments Europe acts as independent Controller for fraud prevention (Art. 6(1)(c) and (f) GDPR); DPA; SCCs for transfers to Stripe Inc.
Anthropic, PBC	USA	Automatic menu translation (Claude API)	Menu texts sent to the «AI Translation» feature	DPA signed; SCCs Module 2; under Anthropic Commercial Terms, API content is not used to train models
Mixpanel Inc.	USA (EU data residency — api-eu.mixpanel.com)	Product analytics (Business Customer events)	Pseudonymous identifiers, app usage events	DPA; EU data residency enabled; SCCs
Vercel Inc.	USA	Hosting and CDN	Technical connection data, HTTP request content	DPA; SCCs; EU region configurable
Lovable	EU	Source code management of the landing page	Read-only repository access	Development engagement; no processing of lead data
Legal, tax and accounting advisors	Italy	Administrative and tax obligations	Billing data	Professional secrecy; Art. 28

Provider	Location	Role	Data	Safeguards
				appointment where applicable

Personal data are not disseminated and are not shared with third parties for their own commercial purposes.

8. International transfers

Some providers listed in section 7 are established in the United States. Transfers rely on:

- **Adequacy decision (Art. 45 GDPR)** of 10 July 2023 on the *EU-US Data Privacy Framework*, for certified providers (e.g., Google LLC);
- **Standard Contractual Clauses (Art. 46(2)(c) GDPR)** approved by Commission Decision 2021/914 (Module 2 — Controller→Processor) for non-DPF-certified providers (Anthropic, Stripe Inc., Vercel, Supabase Inc., Mixpanel);
- **supplementary measures** pursuant to EDPB Recommendations 01/2020: TLS 1.2+ encryption in transit, encryption at rest, pseudonymisation of public menu visitor identifiers, minimisation of data sent to AI APIs.

A copy of the safeguards is available on request at privacy@inasnap.app.

9. Retention period

Data	Retention
Business Customer account (profile, credentials)	For the duration of the contract + 30 days; thereafter deletion or anonymisation, subject to legal obligations
Uploaded content (menus, dishes, translations)	For the duration of the contract; user-deletable from the reserved area; security backups kept for up to 30 days
Billing and accounting documents	10 years pursuant to Art. 2220 Italian Civil Code and tax law

Data	Retention
Security and authentication logs	12 months, with motivated extension for incident handling
Product analytics (Mixpanel)	24 months individually; aggregated indefinitely
Public menu analytics	26 months individually; thereafter aggregation or deletion
Waitlist e-mails	Until launch and first contact, or consent withdrawal; in any case deletion after 24 months of inactivity
Data sent to Anthropic Claude	Anthropic retains up to 30 days on its systems for abuse monitoring
Consent records (Art. 7(1) GDPR)	For as long as needed to demonstrate compliance and in any case no longer than 10 years from revocation or termination

10. Automated decision-making

InASnap **does not carry out solely automated decisions producing legal effects or similarly significantly affecting the data subject** under Article 22 GDPR. AI-assisted menu translation (Claude by Anthropic) is a productivity tool activated upon user request; results are always reviewable and editable by the Business Customer before publication.

11. Security

InASnap adopts appropriate technical and organisational measures under Article 32 GDPR: TLS 1.2+ encryption in transit, encryption at rest on Supabase, password hashing (handled natively by Supabase Auth), role-based access via Row Level Security, staging/production segregation, daily backups, admin access logs, incident management policies and Supervisory Authority notification within 72 hours under Article 33 GDPR where required.

12. Data subject rights

The data subject may at any time exercise rights under Articles 15–22 GDPR:

- **access** (Art. 15); **rectification** (Art. 16); **erasure** (Art. 17, «right to be forgotten»); **restriction** (Art. 18); **portability** (Art. 20); **objection** (Art. 21); **withdrawal of consent** at any time, without affecting prior lawfulness (Art. 7(3)); **right not to be subject to automated decisions** (Art. 22).

Rights are exercised by writing to privacy@inasnap.app. The Controller replies within 30 days, extendable by up to 60 days in complex cases (Art. 12(3) GDPR).

12.1 Right to lodge a complaint

The data subject has the right to lodge a complaint with the **Italian Data Protection Authority** (Garante per la Protezione dei Dati Personali, Piazza Venezia 11, 00187 Roma, www.garanteprivacy.it) or with the supervisory authority of their Member State, under Article 77 GDPR.

13. Cookies and similar technologies

See the **Cookie Policy** at inasnap.app/cookie-policy, which forms an integral part of this notice.

14. Minors

The Services are not intended for persons under 16. InASnap does not knowingly collect data from minors. Any inadvertent processing will be promptly erased upon notice.

15. Changes

The Controller reserves the right to amend this Policy for regulatory, operational or vendor changes. The current version is always available at inasnap.app/privacy-policy with the last update date. For material changes, registered users will be notified by e-mail at least 15 days in advance.