

KULT — Privacy Policy

Last updated: 11 September 2026 · Version 2.0

1. Data controller

The data controller is **KULT S.r.l.**, with registered office at Via della Chiusa 8, Milan, Italy, VAT/tax code [P.IVA – to be completed] ("KULT", "we", "us"). You can contact us on any privacy matter at **privacy@onkult.com** or by post at the address above. [If a DP0 is appointed, add their contact here.]

2. Who this policy applies to

This policy describes how we process the personal data of: (a) applicants and Members of the KULT community who use the "KULT" app (the "App"); (b) people who join our waitlist, visit onkult.com, or interact with our social profiles; (c) contact persons at partner venues and organisers (for whom the partnership agreement also applies); (d) people invited as a guest ("plus-one") by a Member.

3. What data we collect

3.1 Data you give us

When you join the waitlist, apply, or create an account: full name, date of birth (to verify that you are at least 18), e-mail address, phone number, city, Instagram username, one or more photographs (profile/application photo), your interests/vibe tags, answers to application questions, and any other information you choose to add to your profile.

When you request or attend an experience: your preferences and requests, cancellations, attendance and no-shows, and any feedback. When you submit a deliverable: **a screenshot you upload as proof that you published the agreed content** (see 3.2). When you contact us: the content of the communication.

If you invite a guest as a plus-one, we collect the guest's name and, where you invite them by e-mail, their e-mail address, solely to manage that invitation.

3.2 Data about your Instagram profile and content

KULT does **not** use "Sign in with Instagram" and does **not** connect to your Instagram account or access your Instagram credentials or any private content. Instead:

- **You provide your Instagram username** (handle). To assess your application and to calculate your community score and tier, we retrieve information that is **already public** on your Instagram profile — such as follower count, public posts and their public engagement metrics — through a third-party public-data service (see §7, "RapidAPI / Instagram Looter 2"). If your account is private, we cannot retrieve this data and will ask you to make the profile public to be scored; you are free not to.
- **Deliverable verification is screenshot-based, not Instagram-connected.** After an experience, you upload a screenshot of the post or story you published. An automated vision system (see §7, "OpenAI") checks that the screenshot shows the required tag/mention and content. We do not read your Instagram account to verify this.

We do not access private content and never receive your Instagram password.

3.3 Data collected automatically by the App

Device and app identifiers (model, operating system, language, installation identifier), IP address, APNs push-notification token, and server-side request and diagnostic logs (e.g. the endpoints called, errors) that our backend records for security and troubleshooting.

The App contains no third-party advertising, analytics, or cross-app tracking SDKs, does not use an advertising identifier (IDFA), and **does not track you across other apps or websites**. The App **does not collect the device's location**.

3.4 Data received from third parties

From partner venues/organisers: attendance confirmations and feedback about experiences. From Apple/app stores: sign-in confirmation (Sign in with Apple), installation confirmation and, where applicable, aggregated data.

3.5 Special categories of data

We do not ask for special-category data (Article 9 GDPR). Photographs and uploaded screenshots are **not** processed for biometric identification or facial recognition. Please do not include in your application information about health, sexual orientation, political or religious views, or ethnic origin.

4. Purposes, legal bases and retention

Purpose	Data	Legal basis	Retention
Handling your application and selection for the community	Application data (3.1), public Instagram profile data (3.2)	Pre-contractual steps at your request (Art. 6(1)(b))	Rejected application: 12 months; waitlist: until outcome or withdrawal
Creating and managing your account, providing the service, invitations and experiences	Account data, requests, attendance, communications	Performance of the contract (Art. 6(1)(b))	Life of the account + 12 months
Age verification (18+)	Date of birth	Legal obligation and contract (Art. 6(1)(c) and (b))	Life of the account
Community scoring and tiering	Public Instagram metrics (3.2), internal scores	Performance of the contract and legitimate interest in service quality (Art. 6(1)(b) and (f))	Life of the account
Verifying content published for experiences (AI screenshot check), managing no-shows and community quality	Uploaded screenshots, attendance	Performance of the contract and legitimate interest in service quality (Art. 6(1)(b) and (f))	Screenshots deleted/anonymised shortly after the deliverable is settled (approx. 7 days); the verification outcome is kept for the life of the account + 12 months
Sharing with the partner venue/organiser the data needed for the experience	Full name, Instagram username, number of guests, any requests	Performance of the contract (Art. 6(1)(b))	See §6

Purpose	Data	Legal basis	Retention
Push notifications and service communications	APNs push token, e-mail, phone	Performance of the contract (Art. 6(1)(b))	Life of the account
KULT promotional communications (newsletter, new experiences, events)	E-mail, name	Consent (Art. 6(1)(a)); "soft opt-in" under Art. 130(4) Italian Privacy Code for similar communications to existing contacts	Until consent is withdrawn; max 24 months from last interaction
Reposting your content on KULT channels	Content, image, username	Contract/licence accepted in the Terms (Art. 6(1)(b)); consent for further uses	Duration of the licence
Partner subscription billing (partner contacts only)	Billing and contact data (processed via Stripe)	Performance of the contract (Art. 6(1)(b)); legal obligation for invoicing (Art. 6(1)(c))	Statutory accounting periods (up to 10 years)
Diagnostics, security logs and improvement of the App	Automatically-collected data (3.3)	Legitimate interest (Art. 6(1)(f))	14 months, then deleted or aggregated
Security, abuse and fraud prevention, defence of legal claims	All relevant data	Legitimate interest (Art. 6(1)(f))	Up to 10 years for relevant data (ordinary limitation period)
Compliance with legal obligations and authority requests	Relevant data	Legal obligation (Art. 6(1)(c))	Statutory periods

Providing the data marked as mandatory in the App is necessary to apply and use the service; without it we cannot assess your application or provide the service. Consent to promotional communications is optional and does not affect access to the community.

Automated decision-making. Some steps are supported by automated tools:

- **Membership admission** is reviewed by people on the KULT team. Automated tools (age checks, engagement scoring, sorting applications) only support that human review.
- **Selection for a specific experience** is made automatically, ranking eligible applicants and filling limited capacity; the outcome can be to admit, waitlist, or not admit you for that experience.
- **Deliverable verification** is performed automatically by a vision system; where the automated check is inconclusive it is escalated to **human review**, and a Member's standing can be affected (and, at the lower thresholds, an account may be suspended).

Where an automated decision could significantly affect you, you have the right to **obtain human intervention, express your point of view, and contest the decision** by writing to privacy@onkult.com.

5. We do not sell your data

KULT does not sell your personal data and does not disclose it to third parties for their own marketing.

6. Who we share data with

6.1 Partner venues and organisers. When you request an experience we share with the partner only the data strictly necessary to welcome you: full name, Instagram username, number of people and any specific requests. The partner processes that data as an independent controller for guest management, under its undertaking to us to use it only for the experience and to delete it within 30 days.

6.2 Service providers (processors). We use the providers listed in §7, which process data on our behalf under Article 28 GDPR data-processing agreements.

6.3 Instagram / Meta. We retrieve **public** profile data from Instagram via a third-party public-data service (see §7). When you separately publish content on Instagram, that publication happens on Meta's platform under Meta's own privacy policy, which we do not control. We do not connect to your Instagram account and send Meta no data about you.

6.4 Authorities, advisers and corporate transactions. We may disclose data to public authorities where required by law, to legal and accounting advisers bound by confidentiality, and to any acquirer or successor in a merger, acquisition or transfer of business, informing you where required.

7. Providers and transfers outside the EU

Provider	Service	Location / transfer safeguards
Hetzner Online GmbH	Application hosting, database and cache (our primary infrastructure)	Germany (EU) — no transfer outside the EEA
Cloudflare, Inc.	File storage of photos and uploaded screenshots (R2); bot-protection on the waitlist (Turnstile)	EU/USA — EU-US Data Privacy Framework (DPF) and/or Standard Contractual Clauses (SCCs)
Apple Distribution International Ltd	Sign in with Apple (authentication) and iOS push notifications (APNs)	EU/USA — DPF / SCCs
Resend, Inc.	Transactional and magic-link e-mail	USA — SCCs / DPF
RapidAPI (marketplace) and the Instagram Looter 2 API provider	Retrieval of public Instagram profile data from the username you provide	USA — SCCs
OpenAI (OpenAI Ireland Ltd / OpenAI, L.L.C.)	Automated screenshot-based verification of deliverables (vision). API inputs are not used to train models.	EU/USA — DPF / SCCs
Stripe (Stripe Payments Europe Ltd / Stripe, Inc.)	Partner subscription billing (partner contacts only)	EU/USA — DPF / SCCs

Some of these providers may process data on servers located outside the European Economic Area (in particular in the United States). In those cases transfers rely on the EU-US Data Privacy Framework for certified companies or on the Standard Contractual Clauses approved by the European Commission, supplemented where necessary by additional measures. You can request a copy of the relevant safeguards by writing to privacy@onkult.com.

8. Your rights

You have the right to: access your data and obtain a copy; have it rectified; have it erased (e.g. by closing your account); obtain restriction of processing; receive the data you provided in a structured format (portability); object to processing based on legitimate interest and, at any time, to direct marketing; withdraw consent without affecting the lawfulness of prior processing; and not be subject to solely automated decisions that produce legal or similarly significant effects (see §4).

To exercise your rights write to **privacy@onkult.com** or use the features in the App (edit your profile, turn off notifications, unsubscribe from the newsletter via the link in every e-mail, delete your account). We will respond within one month, extendable where the law allows. We may ask you to verify your identity.

You also have the right to lodge a complaint with the Italian Data Protection Authority (**Garante per la protezione dei dati personali**, www.garanteprivacy.it — Piazza Venezia 11, 00187 Rome) or with the supervisory authority of the Member State where you live, or to bring proceedings before the courts.

9. Deleting your account

You can delete your account from the App settings or by writing to privacy@onkult.com. On deletion, profile data is erased or anonymised within 30 days, except data we must keep for legal obligations, to handle disputes, or to prevent re-creation of blocked accounts (kept in minimised form). Content you published on your own social channels remains under your control; reposts on KULT channels will be removed on request within a reasonable time.

10. Security

We apply technical and organisational measures appropriate to the risk, including encryption in transit (TLS) and encryption at rest at our storage providers, role-based access control, secure authentication (magic link and Sign in with Apple, with bearer tokens), access logging and team training. No system is completely secure: if a breach is likely to result in a high risk to your rights, we will inform you as required by Article 34 GDPR.

11. Minors

The App is reserved for people aged 18 or over. We do not knowingly collect data from minors; if we become aware of an account belonging to a minor we close it and delete the data. If you believe a minor has given us data, write to privacy@onkult.com.

12. Cookies and tracking

The App does not use third-party analytics, advertising, or cross-app tracking, and shows no App Tracking Transparency prompt because it performs no tracking. It uses only the technical identifiers and server logs described in §3.3 for the purposes in §4.

The **onkult.com** website uses only technical/essential cookies and similar storage needed for it to function — including a bot-protection challenge (Cloudflare Turnstile) on the waitlist form and standard web-font delivery. [If any non-essential/analytics cookies are added to the website, publish a dedicated cookie policy and link it here.]

13. Changes

We may update this policy. Material changes will be notified through the App or by e-mail before they take effect. The last-updated date appears at the top of this document.