

JUST US

Privacy Policy

English version provided for convenience. The French version ("Politique de Confidentialité") prevails in case of discrepancy.

Data controller: Benoit Cizeron SASU, RCS Nanterre 942 297 763, EUID FR9201.942297763

Privacy contact: privacy@justusapp.co

Version	Date	Changes
1.0	2026-07-22	Initial version, prepared for launch and for Persona production access review.

1. Who we are and scope

This Privacy Policy explains how Benoit Cizeron SASU, registered with the Nanterre Trade and Companies Register under number 942 297 763 (the "Company", "JUST US", "we"), processes personal data when you use the JUST US mobile application and related services (the "Service"). The Company is the data controller.

Contact for privacy matters: privacy@justusapp.co. You can exercise all your rights directly in the App or at this address.

JUST US is designed on a privacy-first, EU-sovereign model: no advertising, no sale of personal data, no tracking for third parties, data hosted in the EU (or in the US at your choice for your account region), identity verification data always hosted in the EU, and AI processing on European infrastructure.

2. Data we collect

2.1 Identity verification data (via Persona)

Before accessing the Service, you complete identity verification operated with our partner Persona Identities, Inc. ("Persona"), acting as our processor. This involves:

- your government-issued identity document (images and extracted data: name, date of birth, document number, nationality, expiry);
- a selfie video/photo with liveness detection, and the biometric facial geometry data derived from it to match your face to your document (processed with your explicit consent, see Section 4);
- verification outcomes and fraud signals (including duplicate detection to enforce one account per person);
- your mobile phone number, verified by one-time SMS code.

2.2 Account and profile data

Verified name, profile information you choose to add, phone number, account region choice (EU or US), Circle memberships and roles, settings.

2.3 Contacts (optional)

If you grant the contacts permission, phone numbers from your address book are hashed on your device and matched against hashed numbers of existing members, so we can suggest Circles where you already know someone. We do not upload your address book in clear form and we do not contact your contacts.

2.4 Content

Signals, Perspectives, direct messages, live session recordings and replays, bookmarks, and your interactions with Aura (queries and outputs). Content is stored in the hosting region of the relevant Circle.

2.5 Usage, device and security data

Device model and OS version, app version, language, identifiers needed for push notifications, log data (timestamps, IP address, actions), security events (authentication, screenshot capture events on protected screens, screen recording detection), and diagnostic data.

2.6 Payment data (when paid services are activated)

When subscriptions or paid Circles become available, payments will be handled by Apple (in-app purchases) or Stripe (marketplace). We receive transaction status and billing metadata, never full card numbers. Owners of paid Circles will additionally provide business verification (KYB) data.

We do not collect your email address for the operation of the Service. JUST US communicates through push notifications, SMS for critical messages, and in-app notices. We never send marketing emails.

3. Why we process your data (purposes and legal bases)

Under the EU/UK General Data Protection Regulation ("GDPR"), we process your data as follows:

- Providing the Service (account, Circles, Signals, messages, notifications): performance of our contract with you (Art. 6(1)(b) GDPR).
- Identity verification and anti-fraud (one verified human per account, anti-bot and anti-deepfake protection): performance of the contract and our legitimate interest in the safety and integrity of a trust-based network (Art. 6(1)(b) and (f)); explicit consent for biometric matching (Art. 9(2)(a)).
- Aura personal AI features (search, bookmarks, digest): performance of the contract, at your initiative when you invoke Aura.
- Contacts matching and Circle suggestions: your consent, through the iOS contacts permission (Art. 6(1)(a)); you can revoke it at any time in your device settings.
- Security, abuse prevention and moderation (including automated scanning for prohibited content and human review): legitimate interest in protecting members and the Service, and compliance with legal obligations, including the EU Digital Services Act (Art. 6(1)(c) and (f)).
- Payments, anti-money-laundering and counter-terrorist-financing checks when paid services are activated: compliance with legal obligations (Art. 6(1)(c)).
- Service analytics and improvement, strictly on our own behalf: legitimate interest; we use aggregated or pseudonymized data wherever possible.
- Legal claims and requests from authorities: compliance with legal obligations and legitimate interest.

We do not profile you for advertising, we serve no ads, and we do not sell or rent your personal data to anyone.

4. Biometric data

Facial geometry data used to match your selfie to your identity document is special-category data under Art. 9 GDPR. It is processed only with your explicit consent, collected before the verification starts. If you refuse, verification cannot be completed and access to the Service is not possible, because verification of every member is the essence of the Service. You may withdraw consent at any time with effect for the future; withdrawal ends your ability to use the Service.

Biometric templates are processed by Persona on our behalf, on EU infrastructure, and are not used for any purpose other than verifying you. Biometric data is deleted in accordance with the retention rules in Section 8 and is never used to train AI models.

5. Aura and AI processing

- Aura is your personal AI. It can read across the Circles you belong to in order to serve you, and its outputs are strictly confined: information from one Circle is never revealed in another Circle or to another member.
- AI processing (including embeddings of Content for search and digest) is performed on European infrastructure by Mistral AI, acting as our processor. Embeddings are stored in the same region as the Content they derive from.
- Your Content and your Aura interactions are not used to train foundation models, whether ours or third parties'.
- Moderation combines automated detection of prohibited content with human review. No decision producing legal or similarly significant effects is taken solely by automated means: identity verification edge cases and moderation appeals include human review, and admission to Circles is decided by humans (Owners and boards), never by an algorithm.

6. Where your data is hosted

- Account and personal AI data: at signup you choose your account region, EU (Paris, AWS eu-west-3) or US (Virginia, AWS us-east-1). This choice is currently not reversible.
- Circle content: hosted in the region chosen by the Circle Owner at creation (EU or US).
- Identity verification data: always hosted in the European Union, for all members, regardless of account or Circle region.
- Encryption: data is encrypted in transit (TLS 1.3) and at rest (AES-256) with keys managed by JUST US (BYOK), meaning our cloud provider cannot decrypt member data on its own.

7. Who we share data with

We share personal data only with processors and partners necessary to run the Service, under contracts complying with Art. 28 GDPR:

- Persona Identities, Inc.: identity verification and fraud prevention (EU data residency for verification data);
- Amazon Web Services (AWS Europe SARL): hosting and infrastructure, EU and US regions as described in Section 6;
- Mistral AI (France): AI processing for Aura;
- Twilio: delivery of SMS (one-time codes, magic links, critical alerts);
- Apple: app distribution, push notifications and, in the future, in-app purchases;

- Datadog: security monitoring and logging;
- Stripe (when the marketplace is activated): payment processing, payouts to Circle Owners, KYB and related AML obligations, for which Stripe acts as an independent controller for certain data.

We may also disclose data where required by law or valid requests from competent authorities, to protect the safety of members (including mandatory reports concerning child sexual abuse material), in connection with legal claims, or in the context of a corporate transaction affecting the Service (such as the planned transfer of the JUST US business to a dedicated entity), in which case protections travel with the data. Circle Owners and Admins see the membership and activity of their Circle within the App, but receive no export of your personal data from us.

8. How long we keep data

- Identity verification data: kept for the duration needed to complete and evidence the verification; after verification, document images and biometric data are purged from our systems in accordance with our agreement with Persona, keeping only the verification result and the minimal audit trail. Where anti-money-laundering rules apply (paid services), applicable data is retained for 5 years as required by law.
- Account and profile data: for the life of the account, then deleted or anonymized after the 30-day soft-delete period following account deletion.
- Content: for the life of the account; upon account deletion, your Signals and Perspectives are anonymized and attributed to "Former member" so conversations keep their coherence. You can delete individual Content at any time before that.
- Contacts matching data: hashed values only, refreshed while the permission is granted, deleted when you revoke the permission or delete your account.
- Logs and security data: up to 12 months, longer only where an incident or legal obligation requires it.
- Payment and billing records (when activated): as required by tax and accounting law (up to 10 years in France).

9. International transfers

If you or a Circle choose the US region, the corresponding data is hosted in the United States as described in Section 6. Where personal data is transferred outside the EEA, the UK or Switzerland, we rely on appropriate safeguards: an adequacy decision where available (including the EU-US Data Privacy Framework for certified providers) and the European Commission's Standard Contractual Clauses, supplemented by encryption with keys held by JUST US and by transfer impact assessments. Identity verification data is not transferred outside the EU.

10. Security

Security measures include: encryption at rest (AES-256, customer-managed keys) and in transit (TLS 1.3, mutual TLS between internal services); isolated network architecture per region; strict least-privilege access with mandatory MFA for our team; secrets management with automatic rotation; continuous security monitoring and logging; vulnerability scanning of code and dependencies; encrypted multi-zone backups; strong member authentication (SMS one-time codes and device biometrics, short-lived sessions with rotating refresh tokens, progressive rate limiting); and anti-leak protections on sensitive screens (author notification on screenshot, dynamic watermarking, blur on screen recording and backgrounding). Our security program is built to align with SOC 2 and ISO 27001 practices, with formal audits planned as the company scales. No system is perfectly secure; we will notify you and the competent authority of any breach as required by Art. 33 and 34 GDPR.

11. Your rights

You have the right to access, rectify and erase your data, to restrict or object to processing, to data portability, and to withdraw any consent at any time (including the biometric consent and the contacts permission) without affecting prior processing. You will not be discriminated against for exercising your rights.

You can exercise these rights directly in the App (Settings, then Privacy) or by writing to privacy@justusapp.co. We answer within one month, extendable as permitted by law. We may need to verify that a request comes from the account holder; because every account is identity-verified, this is normally done in-app without asking you for additional documents.

- EU: you may lodge a complaint with your supervisory authority, in France the CNIL (cnil.fr).
- UK: you may complain to the ICO (ico.org.uk). Switzerland: to the FDPIC.
- US state residents (including California): you have rights of access, correction, deletion and portability as provided by applicable state privacy laws. We do not sell or share personal data for cross-context behavioral advertising, and we honor applicable opt-out rights. Authorized agents may act for you as permitted by law.

12. Minors

JUST US is strictly reserved for adults (18+). Identity verification enforces this rule: age is verified against a government-issued document before any access. We do not knowingly process data of minors; any account found to belong to a minor is terminated and its data deleted.

13. Communications and notifications

JUST US operates without email. We reach you through push notifications (which you can tune per category in the App and in iOS settings), SMS for critical security messages, and in-app notices. We send no marketing emails and no newsletters.

14. Changes to this Policy

We may update this Policy as the Service evolves. Material changes are notified in the App at least 30 days before taking effect, except where changes are required by law or urgent security needs. Where a change relies on consent, we will ask for it. The version history at the top of this document lists all versions.

15. Contact

Benoit Cizeron SASU (JUST US). Privacy contact: privacy@justusapp.co. DSA point of contact: legal@justusapp.co. If we designate a Data Protection Officer, their contact details will be published here and notified to the CNIL.