

DATY.AI PRIVACY POLICY

Consumer Website & Application

Version 1.0

Effective date: 10 September 2026

DATA CONTROLLER

ZeeQuest, Inc. d.o.o., Partizanska cesta 3, Maribor, Slovenia, company registration no. 8402540000, VAT no. 74140841 ("Daty.ai", "we", "us", "our"), is the controller responsible for consumer-facing Daty.ai processing described in this Privacy Policy.

Privacy contact: privacy@daty.ai

Supervisory authority: Information Commissioner of the Republic of Slovenia (Informacijski pooblaščenec)

IMPORTANT

Daty.ai limits the collection and use of personal data to what is necessary for clearly defined purposes. We apply data minimisation, purpose limitation and privacy-by-design principles, particularly to relationship information, AI interactions and information about other people.

Privacy at a glance

- Your account and profile data are used to operate Daty.ai and provide the features you request.
- Compatibility and timing inputs are used to generate Relationship Intelligence outputs. Some inputs may be personal and potentially sensitive depending on what the user provides.
- AI conversations may contain highly personal information. Please do not enter unnecessary sensitive information about yourself or other people in AI conversations.
- Information about another person is a separate privacy risk. Daty.ai will restrict what can be entered and will not treat a user's curiosity as permission to build an unrestricted profile of someone else.
- Marketing is separate from service communications and will use consent or another lawful basis only where applicable law permits.
- Where payments are processed by an authorised payment provider or app store, Daty.ai does not receive or store full payment-card numbers.
- Daty.ai will not sell personal data as a commodity.
- Personal data will not be used to train general-purpose or third-party AI models unless a separate lawful basis, transparency framework and required user controls have been established.

Master Index

1. Scope and Controller
2. GDPR Principles
3. Data We Collect
4. Complete Data-Flow Map
5. Waiting List
6. Account, Registration and SSO
7. Profile and Relationship Intelligence Inputs
8. Information About Another Person
9. AI Conversations and AI Providers
10. Referrals and Pioneer Attribution
11. Location Data
12. Events and Pioneer Hubs
13. Payments and Subscriptions
14. Analytics, Cookies and Device Data
15. Marketing and Communications
16. Customer Support and Feedback
17. Legal Bases
18. Special Categories and Sensitive Information
19. Automated Processing and Profiling
20. Recipients and Processors
21. International Transfers
22. Retention
23. Security
24. Your GDPR Rights
25. Account Deletion
26. Children and Age
27. Changes to this Policy
28. Contact and Complaints

1. Scope and Controller

This Privacy Policy explains how Daty.ai collects, uses, shares, stores and otherwise processes personal data when you use Daty.ai website, waiting list, account, applications, Relationship Intelligence features, AI interfaces, subscriptions, referrals, events, Pioneer-related consumer functionality or support services.

Separate privacy information may supplement this Policy for Pioneer Hubs, business partners, employees, recruitment, specific events or other processing with materially different purposes.

ZeeCapital Ltd (UK) is intended to hold/license Daty.ai intellectual property. Ownership of IP does not by itself make ZeeCapital the controller of consumer personal data. Where ZeeCapital Ltd or another group company receives personal data, its role and the applicable purpose and legal basis are described in this Policy or the relevant product-specific notice.

2. GDPR Principles

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality.
- Accountability and demonstrable compliance.

- Privacy by design and by default, particularly for relationship, AI and third-person data.

3. Data We Collect

Identity/account: Name or display name, email, account ID, age/age confirmation, authentication identifiers, account settings, language, country and SSO identifiers where used.

Profile: Information you choose to provide about yourself, preferences, relationship context, answers to questionnaires/quizzes, profile attributes and settings.

Relationship Intelligence inputs: Data needed for selected compatibility, Natal Engine, Time Engine/ZeRi, CDMA™ or related analyses, which may include birth-related inputs and user-supplied contextual information depending on the feature.

Third-person inputs: Limited information a user supplies about another person for a supported comparison/compatibility feature, subject to strict product rules.

AI interactions: Prompts, questions, conversation text, generated responses, feedback and technical metadata associated with AI features.

Referral: Referral code/link, referring user/Pioneer, invite attribution, conversion events, country/city and reward/eligibility status.

Location: Approximate location inferred from IP/device settings and, only if a feature requires it and permission is obtained, more precise device location.

Events/Hubs: Event registrations, attendance, ticket/booking information, Hub interactions, QR scans/attribution and consented photo/video information where relevant.

Payment/subscription: Plan, amount, currency, transaction/subscription IDs, payment status, billing country and limited payment metadata returned by processors/app stores.

Technical/analytics: IP address, device/browser, operating system, identifiers, timestamps, pages/screens, feature usage, diagnostics, crash/security logs and consented analytics/advertising events.

Marketing: Email/phone where used, consent/preferences, campaign interactions, unsubscribe status and attribution.

Support: Messages, tickets, attachments you choose to provide, account/service context and resolution history.

4. Complete Data-Flow Map

Flow	Main data	Purpose	Legal basis	Retention Period
Waiting list	Email, country, referral, campaign source	Manage pre-launch interest; send requested updates	Consent for marketing; legitimate interest/steps requested where appropriate	12 months from registration or the latest affirmative confirmation, unless you withdraw your consent, unsubscribe or create an account earlier. We delete the data within 30 days after the applicable event, except for a minimal suppression record retained as necessary to honour your opt-out.
Account	Email, ID, age, settings, SSO	Create/authenticate/secure account	Contract; legitimate interest for security	For the duration of the account. After 24 months of inactivity, we may contact you before closing the account. Following closure, operational account data is deleted within 30 days, subject to legal retention requirements and any unresolved dispute.

Flow	Main data	Purpose	Legal basis	Retention Period
Profile	User-entered profile data	Personalise and provide service	Contract; consent where required for optional/sensitive data	For the duration of the account or until you delete the relevant profile information. Following account closure, the data is deleted within 30 days, subject to legal retention requirements.
Compatibility / RI	Inputs, generated scores/reports	Generate requested compatibility/timing analysis	Contract for ordinary data; explicit consent may be required for Art. 9 data	Saved reports and necessary profile inputs are retained for the duration of the account or until deleted by the user. Temporary calculation inputs are deleted within 24 hours where they do not need to be saved. Data is deleted within 30 days after account closure.
Third-person data	Limited comparison inputs	User-requested compatibility comparison	Must be separately validated; legitimate interest is NOT assumed	Limited third-person inputs are processed only for the requested comparison and deleted within 24 hours, including identifiable derived results. Daty.ai does not create persistent profiles of persons who are not users of the Service.
AI conversations	Prompts, responses, feedback	Provide AI Advisor/explanations; safety/security	Contract; legitimate interest for security; separate basis for improvement/training	For 12 months after the last interaction, or until earlier deletion or account closure. Data is deleted within 30 days after a valid deletion request or account closure. Provider-side logs are retained for no longer than 30 days where zero-retention processing is unavailable.
Referral	Codes, attribution, conversion	Attribute invites/rewards; prevent abuse	Contract/program terms; legitimate interest	For 12 months after the last interaction, or until earlier deletion or account closure. Data is deleted within 30 days after a valid deletion request or account closure. Provider-side logs are retained for no longer than 30 days where zero-retention processing is unavailable.
Location	Approximate or permitted precise location	Local content/Hubs/events/features	Legitimate interest for coarse location where appropriate; consent/device permission for precise location	Precise location is processed only while needed for the requested feature, unless you expressly choose to save it. Saved location preferences are retained until you delete them or close your account.
Events/Hubs	Registration, attendance, QR	Administer event/Hub interaction	Contract; legitimate interest; consent for optional marketing/media	Registration, attendance and operational event records are retained for 90 days after the event. Accessibility and dietary information is deleted within 7 days after the event. Payment records are retained for the period required by

Flow	Main data	Purpose	Legal basis	Retention Period
				tax and accounting law.
Analytics	Device/usage events	Measure and improve service	Consent for non-essential analytics; legitimate interest only where legally appropriate/essential	Identifiable or pseudonymous event-level analytics data is retained for up to 2 months. Optional analytics identifiers are retained for up to 6 months, subject to your consent. Aggregated or irreversibly anonymized statistics may be retained for longer.
Marketing	Contact, consent, engagement	Send promotions/news	Consent or applicable e-privacy/direct-marketing basis	Until you withdraw your consent or object to marketing. A minimal suppression record may be retained for as long as necessary to ensure that your marketing preference is respected.
SSO	Provider ID, token, email/name if shared	Authenticate account	Contract	For the duration of the account. Authentication tokens are retained only for their technical validity period and are revoked when the account is closed. Related account data is deleted within 30 days after closure, subject to applicable security and legal requirements.
Payments	Transaction/subscription metadata	Charge, reconcile, refund, prevent fraud	Contract; legal obligation; legitimate interest for fraud	Invoices and supporting tax and accounting records are retained for 10 years after the end of the calendar year to which they relate. Other payment and subscription metadata is retained only for as long as necessary to administer the transaction, resolve disputes and prevent fraud.
Support	Ticket/message /account context	Resolve requests and complaints	Contract; legitimate interest; legal obligation	Routine support requests are retained for 12 months after resolution. Formal complaints are retained for 24 months after final resolution, unless a longer period is necessary due to an ongoing dispute or legal obligation. Identity documents supplied for verification are deleted within 30 days after verification.

* Final legal bases must be validated against the production data map and feature design. A Privacy Policy must describe what Daty.ai actually does, not what it may theoretically do.

5. Waiting List

If you join the Daty.ai waiting list, we process the information requested on the form, such as email address, country and referral/campaign attribution, to register your interest and provide the communications you selected.

Where promotional emails require consent, we obtain and record your explicit consent. Unsubscribing from marketing does not require deletion of a minimal suppression record needed to respect the opt-out.

6. Account, Registration and SSO

When you create an account, we process registration, authentication, age and account-setting information to establish and secure your account and deliver the Service.

If you use Google, Apple, Facebook/Meta or another SSO provider, Daty.ai receives only the categories made available through the selected sign-in flow and permissions. We should request the minimum scopes needed for authentication.

7. Profile and Relationship Intelligence Inputs

Daty.ai processes information you intentionally provide to generate the profile, compatibility, timing and other Relationship Intelligence features your request. When we request a material input, we explain why it is needed at or near the point of collection.

Free-text fields, questionnaires and AI conversations may reveal sensitive information, including information concerning health, sexual orientation, religion, political views or other protected categories. Daty.ai limits collection to data necessary for the selected feature and provides and provides available editing and deletion controls where appropriate.

8. Information About Another Person

This is a high-priority privacy area. A Daty.ai user may wish to compare themselves with another person. That does not create unlimited permission for Daty.ai to collect or retain information about that other person.

Daty.ai restricts information about another person to the minimum required for a supported feature. We do not permit unrestricted dossiers, hidden surveillance, sensitive allegations or unauthorized importing of private third-party information.

Daty.ai does not contact another person merely because a user has entered information about them, unless a separate feature and lawful basis support that contact.

Daty.ai does not permit unrestricted profiling, scraping or hidden surveillance of another person.

9. AI Conversations and AI Providers

When you use an AI feature, we process your prompt and relevant service context to generate a response. Depending on architecture, the prompt or selected context may be sent to contracted AI infrastructure/model providers acting as processors or other appropriately assessed recipients.

Daty.ai does not permit third-party AI providers to use private consumer prompts or personal data to train their general-purpose AI models.

Daty.ai should also not use identifiable private conversations to train its own general-purpose models without a separately documented lawful basis, transparency and appropriate controls.

Safety, abuse prevention and service-quality review may involve limited automated and human review where necessary and disclosed.

10. Referrals and Pioneer Attribution

Referral links may contain an identifier that allows Daty.ai to attribute a visit, registration or qualifying action to the referring user or Pioneer. Daty.ai may process referral events to administer rewards, measure campaigns and prevent fraud.

Referral attribution does not disclose unnecessary personal information between the referrer and the referred person. Where attribution materially affects the referred person, we provide appropriate notice.

11. Location Data

Daty.ai may use coarse location, such as country/city inferred from IP or selected by the user, for localisation, fraud prevention, Hub discovery or event relevance.

If a feature uses precise device location, we request your permission when the feature needs it, explain the purpose and provide a less precise alternative where feasible. We do not continuously collect precise location by default.

12. Events and Pioneer Hubs

If you register for or attend a Daty.ai event, scan a Hub QR code or interact with a Pioneer Hub, we may process registration, attribution, attendance and interaction data needed to deliver the activity and measure the programme.

Photography/video at events requires an appropriate notice and lawful basis. Where we rely on consent for identifiable promotional photographs or videos, you can decline or withdraw that consent through the method communicated for the event. Separate Pioneer Hub business/KYB privacy information may apply to business representatives.

13. Payments and Subscriptions

Payment providers/app stores process payment credentials needed to complete purchases. Daty.ai receive only the payment and subscription metadata needed to administer plans, invoices, refunds, fraud prevention and accounting.

Daty.ai does not need to store full card numbers where an authorised payment provider handles them.

14. Analytics, Cookies and Device Data

Essential technical data may be processed to deliver, secure and troubleshoot the Service. Non-essential analytics, advertising and similar technologies are controlled through the Cookie Preferences in accordance with applicable law.

Rejecting optional tracking must not block core Daty.ai functionality unless the technology is genuinely necessary for the requested service.

15. Marketing and Communications

Service communications needed for account security, transactions, material contractual changes or requested functionality are distinct from promotional marketing.

Where marketing requires consent, Daty.ai will record the consent and provide an easy unsubscribed method. Withdrawal does not affect processing already lawfully carried out before withdrawal.

16. Customer Support and Feedback

We support communications to identify the account, investigate the issue, respond, prevent abuse and maintain an appropriate record of the resolution.

Please do not send unnecessary health, sexual, financial, identity-document or third-person information in support requests unless we specifically request it through a secure process.

17. Legal Bases

- Contract / steps at your request — where processing is objectively necessary to create an account, provide a requested Daty.ai feature, administer a subscription or deliver an event/service.

- Consent — for processing requires freely given, specific, informed and unambiguous consent, including certain marketing, optional device permissions/cookies and potentially special-category processing.
- Legitimate interests — for narrowly defined interests such as service security, fraud prevention, limited product administration or certain analytics only after necessity and balancing have been assessed.
- Legal obligation — for tax, accounting, regulatory, court/order or other obligations imposed on the Operator.
- Vital interests / other GDPR bases — only in exceptional circumstances where legally applicable.

Daty.ai will not use 'legitimate interest' as a blanket basis for Relationship Intelligence, AI development or third-person profiling. We assess the applicable legal basis separately for each material processing purpose.

18. Special Categories and Sensitive Information

Some free-text or relationship-related information may reveal special categories of personal data under Article 9 GDPR, including health information, sexual orientation, religious or philosophical beliefs, political opinions or other protected categories.

Daty.ai does not request special-category information unless a specific feature genuinely requires it and an Article 9 condition has been identified. Where explicit consent is used, it must be separate, specific and withdrawable.

We do not repurpose sensitive information for advertising, unrelated profiling or model training merely because a user disclosed it in a private context.

19. Automated Processing and Profiling

Daty.ai uses automated processing to generate compatibility, timing, profile and AI-based outputs. These outputs are intended as informational/interpretive Relationship Intelligence, not decisions producing legal effects or similarly significant effects about users.

If Daty.ai later introduces solely automated decision-making that produces legal or similarly significant effects, the product and this Policy must be updated before deployment to address applicable GDPR Article 22 safeguards and transparency.

Daty.ai provides meaningful high-level information about the factors and categories used by material profiling features, subject to the protection of trade secrets and platform security.

20. Recipients and Processors

Personal data may be disclosed only where necessary to vetted categories of recipients such as cloud/hosting providers, authentication providers, AI infrastructure/model providers, payment processors, analytics/consent providers, customer-support/CRM systems, communications providers, security/fraud providers, professional advisers and authorities where legally required.

A current list of material subprocessors is available at [\[link\]](#). Group companies do not receive unrestricted access merely because they are affiliates. Group-company access is limited to defined purposes and an applicable legal basis.

21. International Transfers

Some service providers or group companies may be located outside the EEA. Where personal data is transferred internationally, Daty.ai will use an applicable GDPR transfer mechanism, such as an adequacy decision or approved contractual safeguards, together with supplementary measures where required.

22. Retention

Category	Working rule	Final action
Waiting list	Retain for 12 months from	Stop marketing immediately on

Category	Working rule	Final action
	registration or the latest affirmative confirmation of interest , unless the person unsubscribes, withdraws consent or creates an account sooner. Sending emails does not restart the period.	unsubscribe. Delete the waiting-list record within 30 days of expiry, withdrawal or migration. Keep only a minimal suppression record while needed to prevent renewed unwanted contact; review annually.
Account/profile	Retain while the account is active. Review accounts after 24 months without user activity , excluding ongoing paid subscriptions or unresolved transactions.	Give inactive users 30 days' notice before closure. On closure or a valid deletion request, remove the profile from visibility immediately and delete operational personal data within 30 days . Keep necessary security logs for 90 days from creation .
RI inputs/reports	Retain saved Relationship Intelligence reports and essential profile inputs while needed for the active account. Delete temporary calculation inputs within 24 hours after successful processing .	Provide controls to delete individual reports and associated inputs. Complete deletion within 30 days , including derived profiles and embeddings where applicable. Account closure triggers deletion of remaining history.
Third-person inputs	Default to session-only processing , with deletion no later than 24 hours after processing , including identifiable derived results. Do not build persistent profiles of non-users by default.	Exclude these inputs from routine logs, backups and model training. Complete the DPIA, lawful-basis assessment and Article 14 assessment before enabling the feature. Short retention does not remove these obligations.
AI conversations	Retain conversation history for 12 months from each conversation's last interaction , or until earlier user deletion/account closure. Keep routine security metadata for 90 days from creation .	Provide conversation deletion controls and complete deletion within 30 days . Require zero provider content retention where available , otherwise a verified maximum of 30 days for routine provider logs. Disable provider model training; document any exceptions before use.
Payments	For Slovenian invoicing, retain invoices and required supporting tax records for 10 years after the end of the relevant calendar year , subject to confirmation of the applicable record category. Do not apply this period to the entire user profile.	Separate the finance archive from operational account data and restrict access. Retain transaction references rather than full card details; never retain CVV codes . Have the accountant confirm the entity-specific schedule and any longer statutory requirements.
Referral	Proposed attribution window: 90 days	Align the window with the Referral Terms before adoption. Delete

Category	Working rule	Final action
	from the qualifying referral click. Delete unmatched tracking data at expiry. Keep minimal successful referral and reward records while rewards remain active, then 24 months after final settlement for disputes/fraud review where justified.	unnecessary device/IP data within 90 days . Apply the payments schedule only to reward records that qualify as accounting evidence.
Analytics	Retain identifiable or pseudonymous event-level analytics for 2 months from collection . Use a maximum 6-month lifetime for optional analytics identifiers, subject to consent requirements.	Configure each tool and consent-management platform accordingly. Stop optional collection on withdrawal. Keep longer-term statistics only when irreversibly anonymized , not merely pseudonymized.
Support	Retain routine support tickets for 12 months after resolution . Retain formal complaint records for 24 months after final resolution , unless a documented legal hold applies.	Delete identity-verification attachments within 30 days after verification , unless specifically required longer. Redact unnecessary sensitive information. Retain only the relevant extracts for an active dispute.
Event	Retain registration, attendance and event logistics records for 90 days after the event . Delete accessibility/dietary information within 7 days after the event , unless needed for a documented incident. Finance records follow the payments schedule.	Delete unused raw photos/video within 90 days . Review selected promotional media after 24 months and remove it unless continued use has a documented purpose and lawful basis. Handle consent withdrawal and objections under the event media policy.

Data will be deleted or irreversibly anonymised when no longer needed, subject to lawful retention obligations.

23. Security

Daty.ai will use technical and organisational measures appropriate to the risks, including access controls, authentication, encryption where appropriate, logging, environment separation, backups, vulnerability management, vendor controls, incident response and staff confidentiality/training.

No online service can guarantee absolute security. Users should protect their credentials and report suspected compromise promptly.

24. Your GDPR Rights

- Access — obtain information and a copy of personal data, subject to applicable limits.
- Rectification — correct inaccurate or incomplete personal data.
- Erasure — request deletion where GDPR conditions apply.
- Restriction — request restriction of processing in specified circumstances.
- Portability — receive qualifying data in a structured, commonly used, machine-readable format.
- Object — object to processing based on legitimate interests in appropriate circumstances; object to direct marketing at any time.

- Withdraw consent — where processing relies on consent, without affecting prior lawful processing.
- Rights concerning solely automated decisions with legal or similarly significant effects, where Article 22 applies.
- Lodge a complaint with a competent supervisory authority, including the Slovenian Information Commissioner where appropriate.

Requests: privacy@daty.ai. Daty.ai may need to verify identity proportionately before fulfilling a request. Rights are not absolute and lawful exemptions may apply.

25. Account Deletion

Daty.ai provides an accessible account-deletion mechanism. When you delete your account, we delete or anonymise personal data that is no longer required, subject to applicable retention obligations.

Deleting an account does not require Daty.ai to erase data that must lawfully be retained, nor data that has been irreversibly anonymized.

26. Children and Age

Daty.ai is intended exclusively for individuals aged 18 or older. We do not knowingly create consumer accounts for individuals under 18.

27. Changes to this Policy

We may update this Policy when products, vendors, laws or processing change. Material changes will be communicated as required. Previous versions may be retained for transparency and accountability.

28. Contact and Complaints

Controller: ZeeQuest, Inc. d.o.o.

Registered office: Partizanska cesta 3, Maribor, Slovenia

Privacy: privacy@daty.ai

Support: support@daty.ai

You have the right to lodge a complaint with the competent data protection authority, in particular in the EU Member State of your habitual residence, place of work or the place of the alleged infringement. The supervisory authority in Slovenia is the Information Commissioner of the Republic of Slovenia (Informacijski pooblaščenec), Dunajska cesta 22, 1000 Ljubljana, Slovenia, gp.ip@ip-rs.si, www.ip-rs.si.