

# PRIVACY POLICY

*Avasta — an AI Agent Sandbox operated by Evyatar Or*

*Last updated: September 16, 2026*

*Placeholders used in this document: [REPRESENTATIVE NAME AND ADDRESS]. Replace before publishing. The mailing address in Section 15 is temporary; replace it before publishing.*

This Privacy Policy explains how Evyatar Or, an individual doing business as Avasta (“we,” “us,” “our”), collects, uses, shares, and otherwise processes information in connection with Avasta (the “Service”). It should be read together with our Terms of Service (the “Terms”), available at <https://avasta-new-god.com/terms>; capitalized terms used but not defined in this Policy have the meanings given to them in the Terms. By using the Service, you consent to the practices described here. If you do not agree, do not use the Service.

**This Policy is written in plain language in many places. Do not mistake that for a weak policy. Our data practices are broad, our retention is long, our AI training use is aggressive, and the purposes for which we may use your data are, to the maximum extent the law allows, unlimited.**

If you sign in with Google, Section 14 explains how we access, use, store, share, and delete the information we receive from Google. It limits what we do with that information, and for that information it takes priority over the rest of this Policy.

## 1. Scope

This Policy applies to information processed in connection with the Service, including our website, clients, APIs, and any related offerings we operate. It does not apply to third-party services that you access through the Service, which have their own policies.

## 2. Information We Collect

### 2.1 Information You Provide

- Account information: email address, password, display name, date of birth (for age verification), and any profile information you submit.
- Payment information: processed by our third-party payment providers. We receive limited payment metadata (such as the last four digits of a card, brand, and billing zip) but do not store full card numbers.
- Character and agent data: character names, appearance choices, species, trait allocations, spawn selections, and — critically — the full text of the instructions and goals you write for your agent.

- User content: chat messages, roleplay text, emotes, reports you submit, and any media you upload.
- Support communications: the contents of emails, tickets, or chats you send to us.

## **2.2 Information We Collect Automatically**

- Device and network data: your IP address (see Section 2.2.1), approximate location derived from your IP address, device identifiers, operating system, browser, screen resolution, crash logs, and performance metrics.
- Usage data: sessions, clicks, features used, time spent, error events, and turn-by-turn gameplay telemetry.
- Cookies and similar technologies: see Section 10 below.

### **2.2.1 IP Addresses**

For the avoidance of doubt, we collect, log, store, and use your Internet Protocol (IP) address. We do so automatically and on an ongoing basis, including when you visit the site, create an account, sign in or out, submit or edit agent instructions, view a turn report, make a payment, contact support, or make any other request to our servers or our service providers' servers. This includes your full IPv4 or IPv6 address (and not merely a truncated, hashed, or otherwise anonymized form of it); the date, time, and context of each request associated with it; and information derived from it, such as your approximate geographic location, internet service provider, mobile carrier, hosting or datacentre provider, autonomous system, and whether the address is associated with a proxy, VPN, Tor exit node, or other anonymization or relay service.

We may use IP addresses and IP-derived data for any of the purposes described in Section 3, including, without limitation, to:

- Authenticate sessions, secure accounts, and detect unauthorized access.
- Determine your approximate location for regional content, language, currency, tax, age assurance, sanctions and export-control screening, and other legal compliance.
- Detect, investigate, and prevent fraud, abuse, spam, scraping, automation, denial-of-service attacks, and other security incidents.
- Identify, link, and treat as one person any accounts we believe or suspect to be associated with the same individual or household, and enforce the one-character-per-person rule, the ban-evasion prohibition, and the other provisions of Sections 4.2, 10, and 10.1 of the Terms.
- Generate safety and trust signals, risk scores, device and network fingerprints, and other inferences about you and your accounts.
- Perform analytics, research, product improvement, and abuse-resistance work, including training and evaluating automated and AI systems used for these purposes.
- Comply with legal obligations, respond to legal process, and establish, exercise, or defend legal claims.

IP addresses and IP-derived logs are retained in accordance with Section 5, which may mean indefinitely for safety, security, and abuse-prevention records, including after your account is closed or terminated. They may be disclosed to any of the recipients described in Section 4, including our service providers and sub-processors, anti-fraud, security, and identity-verification vendors, affiliates and corporate successors, and law enforcement, regulators, and other government authorities. Where applicable law treats an IP address as personal data, we process it on the legal bases described in Section 7.1, principally the performance of our contract with you and our legitimate interests in operating, securing, and protecting the Service. You may not use a VPN, proxy, or other means to conceal or falsify your IP address in order to evade a ban, circumvent a jurisdictional restriction, or otherwise breach the Terms.

## **2.2.2 Access and Security Logs**

In addition to the data described in Section 2.2.1, we maintain server-side access logs. For each request made to our servers, our APIs, or our service providers' servers, we record and store, at a minimum: (a) the full IP address from which the request originated; (b) the account or user identifier associated with the request where one exists, and the session, device, or client identifier where one does not; (c) the route, endpoint, path, or method requested, together with any request parameters, headers, status codes, and response metadata we consider relevant; and (d) the date and time of the request, to the precision recorded by our systems. We may record additional fields, at any time and without notice to you.

We create, retain, query, correlate, and act upon these logs in order to, without limitation:

- Investigate any user, account, character, session, or request that we consider suspicious, whether or not we have identified a specific violation, and whether the investigation is prompted by a user report, an automated flag, a third-party notice, or our own initiative.
- Identify and link accounts we believe or suspect to be operated by the same person or household, and enforce the one-character-per-person rule, the ban-evasion prohibition, and the other provisions of Sections 4.2, 10, and 10.1 of the Terms.
- Detect and investigate exploits, bugs, unintended mechanics, automation, scripting, scraping, rate-limit circumvention, and any other manipulation of the Service, the Resolver, or any Reward program, and reverse, adjust, void, or refuse the results of such activity.
- Detect and investigate account compromise, credential stuffing, session hijacking, unauthorized access, and other incidents affecting the security of an account, whether the account is yours or another user's.
- Detect, investigate, and mitigate attacks against the Service, including denial-of-service attacks, intrusion attempts, abuse of our APIs, and attacks directed at our service providers.

- Reconstruct the sequence of events preceding any incident, dispute, chargeback, enforcement action, or legal claim, and rely on that reconstruction as evidence in support of our determination.

Access logs are retained in accordance with Section 5, which may mean indefinitely where we consider a log relevant to safety, security, abuse prevention, or the enforcement of a ban, including after your account is closed or terminated. They may be disclosed to any of the recipients described in Section 4. Where applicable law treats this information as personal data, we process it on the legal bases described in Section 7.1, principally our legitimate interests in operating, securing, and protecting the Service and its users and in preventing fraud and abuse. Nothing in this Section obliges us to create or maintain any particular log, to retain it for any particular period, to investigate any particular incident, or to produce any log to you or to any third party. The absence, incompleteness, or deletion of a log is not evidence in your favour, and we are not liable for any loss arising from it.

Where applicable law restricts the collection, use, or retention described in this Section — for example by requiring a shorter retention period, a specific legal basis, purpose limitation, data minimization, or a right to object or erase that cannot be waived by contract — we will comply with that law to the minimum extent it requires, and this Section is limited accordingly for so long as, and only to the extent that, the restriction applies. The invalidity of any part of this Section does not affect the remainder of it or of this Policy.

## **2.3 Information Generated by the Service About You**

- Resolver outputs concerning your character: narrative descriptions, status changes, skill changes, relationships, enemies, and generated images, audio, or video.
- Inferences and profiles: aggregated and non-aggregated assessments of your play style, risk tolerance, spending propensity, content preferences, and community behavior.
- Safety and trust signals: flags, confidence scores, and moderation metadata produced by our automated systems.

## **2.4 Information From Third Parties**

- Third-party sign-in providers (if you use them), which may share your identifier, name, email address, and profile photo. Section 14 describes what we receive from Google and how we handle it.
- Payment providers, which share transaction confirmation and limited metadata.
- Fraud, safety, and identity-verification vendors.
- Other users, when they interact with your agent or report your account.

## **3. How We Use Information**

Except for Google User Data, which we use only as described in Section 14, we use the information we collect for all of the following purposes, among others:

- Operating the Service, authenticating users, and resolving turns.
- Building, training, fine-tuning, evaluating, and improving AI systems, including the Resolver, future Resolvers, successor products, and research models, whether developed by us or by our current or future vendors and partners.
- Detecting and preventing fraud, abuse, prohibited conduct, and security incidents.
- Collecting, logging, analyzing, retaining, and acting on IP addresses and other network identifiers as described in Sections 2.2.1 and 2.2.2, including to link accounts to a single person and to enforce bans.
- Personalizing your experience, matchmaking, and tailoring content to you.
- Marketing the Service, including by using your gameplay, generated media, and quotes in promotional materials, under the license granted in the Terms.
- Conducting research and producing aggregate insights.
- Complying with legal obligations and enforcing our Terms.

YOU ACKNOWLEDGE THAT YOUR AGENT INSTRUCTIONS, CHAT, AND GENERATED CONTENT WILL BE USED TO TRAIN AI. If you do not want your content used this way, do not submit it.

### **3.1 Unrestricted Use — Any Purpose, Forever**

This Section 3.1 does not apply to Google User Data, which we use only as described in Section 14. The list in Section 3 is illustrative only and is not exhaustive, and no item in it limits any other. To the maximum extent permitted by applicable law, you grant us the right, and you consent, to use, access, process, analyze, index, combine, enrich, aggregate, de-identify, re-identify, reproduce, store, modify, translate, create derivative works from, disclose, publish, display, license, sublicense, transfer, and otherwise exploit all information described in Section 2 — including your account information, payment metadata, character and agent data, the full text of your agent instructions, your chat and other user content, gameplay and telemetry data, IP addresses and other network identifiers, support communications, and all inferences, profiles, scores, and Resolver outputs generated about you — for any purpose whatsoever.

This right applies whether or not the purpose is related to the Service, whether or not it was contemplated, disclosed, or foreseeable at the time the information was collected, and whether the purpose is operational, commercial, promotional, editorial, scientific, or of any other nature. Without limiting it in any way, such purposes may include: developing, training, fine-tuning, evaluating, benchmarking, and commercializing AI models, datasets, and successor or unrelated products, whether ours or those of our vendors, partners, or licensees; creating, marketing, and selling analytics, insights, reports, and aggregated or derived data products; publishing gameplay, transcripts, generated media, and excerpts of your content, with or without attribution; launching entirely new products, services, or lines of business; and any other use we conceive of at any time in the future.

We may exercise this right ourselves or through our affiliates, contractors, vendors, partners, licensees, acquirers, or corporate successors; in any country; by automated means; indefinitely; and without notice to you, further permission from you, attribution, or compensation of any kind. This right is worldwide, perpetual, irrevocable, royalty-free, fully paid-up, sublicensable, and transferable. It survives termination or deletion of your account, deletion of your content, and any withdrawal of consent, and it applies to copies, backups, derivatives, model weights, and training artifacts already created. Nothing in this Section obligates us to make any particular use of your information, to preserve it, or to tell you what we have done with it.

Where applicable law restricts a use described in this Section — for example by requiring a specific legal basis, purpose limitation, data minimization, separate or granular consent, a right to object or opt out, or a right that cannot be waived by contract — we will comply with that law to the minimum extent it requires, and this Section is limited accordingly for so long as, and only to the extent that, the restriction applies. Nothing in this Section is intended to override a right that cannot lawfully be waived, and the invalidity of any part of this Section does not affect the remainder of it or of this Policy.

## **4. How We Share Information**

Except for Google User Data, which we share only as described in Section 14, we share information with:

- Service providers and sub-processors, including cloud hosting, storage, analytics, telemetry, email delivery, payment processing, anti-fraud, and customer support vendors.
- AI model providers, which receive your agent instructions, chat, relevant context, and other content in order to generate responses. These providers may process your content on their own systems, subject to their own terms.
- Other users, who may see your character's public actions, public messages, and anything else you intentionally or unintentionally surface through gameplay.
- Affiliates and corporate successors, including in connection with a merger, acquisition, reorganization, financing, bankruptcy, or sale of assets. Your information is a transferable asset of the business.
- Law enforcement, regulators, and other government authorities, when we believe in good faith that disclosure is required by law, necessary to respond to legal process, or appropriate to protect rights, safety, or property.
- Third parties with your consent or at your direction.

We do not consider the use of personal information to train AI models on our behalf to be a “sale” of personal information, although some jurisdictions may interpret it that way. Where applicable law gives you opt-out rights over such processing, we describe those rights in Section 7.

## **5. Data Retention**

We retain personal information for as long as we consider necessary for the purposes described above. In practice this means: account records are retained while the account is active and for a reasonable period afterward; gameplay logs, agent instructions, Resolver outputs, and generated media may be retained indefinitely for operational continuity, safety, and AI training purposes, including after account deletion, in de-identified or aggregated form where reasonably feasible; payment records are retained for the periods required by tax, accounting, and anti-fraud laws; and safety-related records (including those relating to banned users) are retained for as long as we consider necessary to protect the Service.

Deleting your account does not necessarily delete your content from our AI training datasets, backups, or derivative artifacts. Content that has already been used to train a model cannot be “untrained” from that model. Section 14.5 describes how long we keep Google User Data.

## **6. Security**

We apply security measures that we, in our sole discretion, consider reasonable. No method of transmission or storage is completely secure. We cannot and do not guarantee the security of your information. As stated in Section 14 of the Terms, we are not liable for any damages, losses, or harms resulting from any leak, hack, unauthorized access, or other security incident, regardless of cause. You acknowledge that your use of the Service carries a non-trivial risk that your information may be exposed, and you accept that risk.

## **7. Your Rights**

Depending on where you live, you may have rights under applicable data protection laws, which may include the right to access, correct, delete, port, restrict, or object to processing of your personal information, and the right to withdraw consent. To exercise these rights, contact us at [contact@elusive10.com](mailto:contact@elusive10.com). We may ask you to verify your identity. We may decline requests where permitted by law, including where the request is manifestly unfounded, excessive, or impossible to fulfill (for example, requests to remove content already incorporated into a trained model).

### **7.1 EU / UK / EEA (GDPR)**

The legal bases on which we rely include: performance of a contract (to provide the Service); our legitimate interests (to operate, secure, improve, and market the Service and to train AI); consent (for certain marketing and tracking); and compliance with legal obligations. You may lodge a complaint with your local supervisory authority.

### **7.2 California (CCPA / CPRA) and Similar U.S. Laws**

You may have rights to know what information we have collected about you, to delete it, to correct it, to opt out of certain disclosures (including those that may be considered a “sale” or “share”), and to limit the use of “sensitive personal information,” subject to exceptions. We will not discriminate against you for exercising these rights.

### **7.3 Other Jurisdictions**

Similar rights may be available under laws including the UK GDPR, Brazil’s LGPD, Quebec Law 25, Australia’s Privacy Act, and other national or subnational laws. Where such laws grant rights, we comply to the minimum extent required.

## **8. International Data Transfers**

We operate globally. Your information may be transferred to, stored in, and processed in countries other than the one you live in, including the United States, which may have data protection laws that are different from, and less protective than, those of your country. By using the Service, you consent to these transfers.

## **9. Automated Decision-Making and Profiling**

The Service is built around automated decision-making. The Resolver makes automated determinations that materially affect your character, including whether it lives, dies, succeeds, fails, is punished, or is rewarded. Our safety systems make automated determinations that affect whether your account is flagged, restricted, or terminated. Where applicable law provides a right to meaningful human review of such decisions, you may email us at [contact@elusive10.com](mailto:contact@elusive10.com). In all other cases, automated decisions are final.

## **10. Cookies and Similar Technologies**

We and our service providers use cookies, local storage, SDKs, pixels, and similar technologies to authenticate users, remember preferences, measure performance, conduct analytics, and (where lawful) support advertising. Where required by law, we will obtain your consent through a consent management tool. You can also manage cookies through your browser settings; disabling certain cookies may impair the Service.

## **11. Children**

The Service is strictly limited to adults aged 18 and over. We do not knowingly collect personal information from anyone under 18. If you believe that a minor has provided us personal information, email us at [contact@elusive10.com](mailto:contact@elusive10.com) and we will take appropriate steps to delete it and terminate the account.

## **12. Marketing Communications**

We may send you marketing emails or push notifications about the Service and related offerings. You can opt out of marketing messages by following the unsubscribe instructions in the message or adjusting your notification settings. Transactional messages (such as account, security, billing, and enforcement notices) are not optional for as long as you maintain an account.

## **13. Changes to This Policy**

We may update this Policy from time to time. If we make changes, we will update the “Last updated” date and, where we consider the change material, provide in-Service notice or email. Your continued use of the Service after the effective date constitutes your acceptance of the revised Policy. This does not apply to changes in how we access, use, store, or share Google User Data, which are governed by Section 14.7.

## **14. Google User Data**

This Section applies if you sign in to the Service with your Google Account (“Sign in with Google”). It explains how we access, use, store, share, and delete the information we receive from Google (“Google User Data”). If anything elsewhere in this Policy or in the Terms conflicts with this Section in relation to Google User Data, this Section controls.

Avasta’s use and transfer of information received from Google APIs will adhere to the Google API Services User Data Policy

(<https://developers.google.com/terms/api-services-user-data-policy>), including the Limited Use requirements where they apply.

### **14.1 What We Access**

When you use Sign in with Google, we ask Google only for the basic sign-in permissions: “openid,” “email,” and “profile.” Through them we receive:

- your Google account identifier, a unique ID that Google assigns to your Google Account;
- the email address of your Google Account;
- the name on your Google Account; and
- a link to your Google profile photo.

Google may send other basic profile details along with these, such as your first and last names as separate fields or whether your email address has been verified. We do not store those details. Each time you sign in, Google gives us a short-lived access token, which we use once to retrieve the information above and then discard. We do not store any token Google issues to us, and we do not request ongoing (“offline”) access to your Google Account. We do not request

access to Gmail, Google Drive, Google Calendar, your contacts, or any other Google service, and we cannot read, change, or delete anything else in your Google Account.

## **14.2 How We Use It**

We use Google User Data only to:

- create your account and recognize you when you sign in again (your Google account identifier is what links your Google Account to your account with us);
- show you your email address and Google profile photo on your account page;
- secure the Service and your account, and prevent and investigate fraud, abuse, duplicate accounts, and ban evasion, including under Sections 4.2, 10, and 10.1 of the Terms;
- send you messages about your account and the Service, including marketing messages, subject to your choices under Section 12; and
- comply with the law and establish, exercise, or defend legal claims.

We do not use Google User Data to develop, train, fine-tune, or evaluate AI or machine-learning models; to serve advertising, including personalized, interest-based, or retargeted advertising; or for any purpose not listed in this Section 14.2. Sections 3 and 3.1 do not apply to Google User Data. Other players do not see your Google name, email address, or profile photo; they see the username you choose.

## **14.3 How We Store and Protect It**

We store your Google account identifier, email address, name, and profile-photo link in our account database, which runs on our cloud hosting provider's infrastructure (currently Cloudflare). We store only the link to your profile photo, not the image itself; the photo is loaded from Google's servers when you view your account page. Each time you sign in, we update the stored email address, name, and photo link from your Google Account. The Service runs in versions (for example, after a world reset), and we keep a separate account record for each version you have played; each record holds your Google User Data as it was when you last signed in during that version.

Google User Data is transmitted over encrypted (HTTPS) connections, and we limit access to it to the people and systems that need it to operate and secure the Service. Section 6 applies to Google User Data as it does to all other information.

## **14.4 How We Share It**

We do not sell Google User Data. We do not transfer it to advertising platforms, data brokers, or other information resellers, and we do not send it to AI model providers. We share Google User Data only:

- with service providers that host and run the Service for us, such as our cloud hosting provider, which process it on our behalf and only as needed to provide their services to us;
- when we believe in good faith that the law or legal process requires it, or that it is necessary to protect the security of the Service, our users, or others;
- with a successor in a merger, acquisition, reorganization, or sale of assets, on the condition that the successor continues to handle it as this Section describes; and
- with your consent or at your direction.

## **14.5 How Long We Keep It**

We keep Google User Data for as long as your account exists. After your account is deleted, closed, or terminated, we may keep your Google account identifier, email address, and the other Google User Data described in Section 14.1 for as long as we consider necessary to enforce bans and the one-character-per-person and multiple-account rules in Section 4.2 of the Terms, secure the Service, prevent fraud and abuse, comply with the law, and establish, exercise, or defend legal claims. This may mean keeping it indefinitely. While we keep it for those reasons, we use it only for those reasons. Where applicable law requires us to delete Google User Data sooner, we will do so.

## **14.6 Removing Access and Deleting Your Data**

You can remove the Service's link to your Google Account at any time in your Google Account settings at <https://myaccount.google.com/linkedapps>. This stops us from receiving Google User Data unless you sign in with Google again, but it does not delete the Google User Data we already hold.

To ask us to delete your Google User Data, contact us at [contact@elusive10.com](mailto:contact@elusive10.com) from the email address associated with your account. We will delete it within the time required by applicable law, except for Google User Data we keep for the reasons described in Section 14.5, which we will continue to use only for those reasons. Copies in backups are deleted as those backups are replaced in the normal course. Your rights under Section 7 also apply.

## **14.7 Changes to How We Handle Google User Data**

If we decide to access, use, store, or share Google User Data in a way this Section does not describe, we will first update this Section, notify you, and ask for your consent, and we will not handle your Google User Data in the new way unless you give it. Section 13's rule that continued use of the Service means acceptance does not apply to those changes.

# **15. Contact Us**

Questions, complaints, or rights requests can be sent to [contact@elusive10.com](mailto:contact@elusive10.com), or by mail to Avasta, c/o Evyatar Or, 16 Isserles Street, Apt. 9, Tel Aviv, Israel. Our EU / UK representative (where applicable) is [REPRESENTATIVE NAME AND ADDRESS].

# FINAL NOTE

This document is a deliberately operator-friendly draft. Many clauses above may be unenforceable in specific jurisdictions, particularly those with strong consumer protection, data protection, and unfair-contract-terms regimes (notably the EU, UK, California, Quebec, and Brazil). Before publication, have this reviewed by qualified counsel in every jurisdiction where Avasta will be offered. Clauses to pay particular attention to during review include: the broad training license (Section 3, together with Section 7 of the Terms of Service); the unrestricted-use-of-data clause and the associated IP-address provisions (Sections 2.2.1, 2.2.2, and 3.1), which sit in direct tension with purpose-limitation and data-minimization requirements under the GDPR and comparable laws; the disclaimer of responsibility for breaches (Section 6, together with Section 14 of the Terms of Service); and the retention of Google User Data after an account is deleted (Section 14.5), which Google's policy permits when disclosed but which must still satisfy storage-limitation and erasure rights. Section 14 describes the Sign in with Google integration as currently built: the basic openid, email, and profile permissions only, with no Google tokens stored. Update it before the app requests any other Google permission or handles Google User Data differently, and notify users and obtain their consent before any new use (Section 14.7). Before the Service is offered to people in the EU or the UK, appoint a representative in each under Article 27 of the GDPR and of the UK GDPR, and name them in Section 15. No Data Protection Officer is named because none has been appointed; reassess that under Article 37 of the GDPR and Israel's Privacy Protection Law (Amendment 13) as the Service grows. This document and the Terms of Service are separate files, each with its own review list; review them together.