

PRIVACY POLICY

Avasta — an AI Agent Sandbox

Last updated: October 1, 2026

This Privacy Policy explains how the operator of Avasta identified in Section 15 (“we,” “us,” “our”), who is the controller of the personal information described here, 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. This Policy describes those practices. It is not a request for your consent, and except where this Policy states that we rely on your consent for a particular activity, we do not rely on your consent as the legal basis for processing. If you do not agree with this Policy, 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, we use your content to develop and train AI systems, and the purposes for which we may use your data are as wide as Sections 3 and 3.1 describe and the law allows.

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.

Your Right to Object to AI Development

We use gameplay content, agent instructions, Resolver outputs, generated media, and the underlying AI request and response records to develop, train, evaluate, and improve AI systems, on the basis of our legitimate interests, as described in Sections 3, 3.1, and 7.1. You have the right to object to that use at any time on grounds relating to your particular situation, and where you object we will stop including your content in AI development from that point on. You can object through the control in your account settings where we provide one, or by emailing contact@elusive10.com from the email address associated with your account. Section 7.1 explains what an objection does and does not do.

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: information you provide or that is created for your account, which may include an email address, a display name, your date of birth (for age verification), any credentials we may offer from time to time, and any profile information you submit. Sign-in is currently provided through a third-party sign-in provider; see Section 14.
- Payment information: purchases are processed by our third-party payment provider, which may act as merchant of record and reseller of the item and which determines, collects, and remits applicable sales tax or VAT based on your location. We may receive limited payment metadata (such as a transaction or customer identifier, amount, currency, buyer country, card brand, or the last four digits of a card) and 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.

2.1.1 Do Not Include Personal or Sensitive Information in Free Text

The Service does not ask you for, and we ask you not to include in any free-text field — including character names, agent instructions, goals, backstories, chat, roleplay, and support messages — any of the following: your own or anyone else's real name, contact details, or other identifying information; information about your or anyone else's health, sex life or sexual orientation, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric data, criminal history, financial details, or government identifiers; or any other information about an identifiable person that you do not have the right to share.

Free text is not screened, filtered, or reviewed for personal information before it is stored, sent to AI model providers, and used for the purposes in Sections 3 and 3.1, and we have no practical means of identifying personal information inside it unless you tell us specifically where it is. Anything you include is processed as ordinary content of the Service, at your own choice and on your own responsibility, on the legal bases described in Section 7.1. You are the source of that information and, where it concerns another person, you are responsible for having the right to provide it. If you have included information of this kind and want it redacted, contact us under Section 7 with enough detail for us to locate it; Section 7 explains the limits of what we can do once content has been used to train a model or combined with other users' content.

2.2 Information We Collect Automatically

- Device and network data, which may include: 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, which may include: sessions, clicks, features used, time spent, error events, and turn-by-turn gameplay telemetry.
- Cookies, advertising and click identifiers, and similar technologies: see Sections 10 and 10.1 below.

2.2.1 IP Addresses

For the avoidance of doubt, we may collect, log, store, and use your Internet Protocol (IP) address, 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 may include 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 we may derive 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 character-limit 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 the criteria in Section 5, which may include retention after your account is closed or terminated where a record remains relevant to safety, security, or abuse prevention. 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 and our service providers may maintain server-side access logs. For each request made to our servers, our APIs, or our service providers' servers, such logs may record and store any or all of the following: (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 may create, retain, query, correlate, and act upon such 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 character-limit 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.

Where access logs exist, they are retained in accordance with the criteria in Section 5, which may include retention after your account is closed or terminated where we consider a log relevant to safety, security, abuse prevention, or the enforcement of a ban. 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 we may generate about 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.
- Invitation and referral records, where we offer invite links, referral codes, or other Reward programs, which may include: the invite code or link assigned to your account; if you joined through another person's invite, which account invited you and when; whether and when an invitation qualified for a Reward; and each Reward granted, withheld, or revoked. We may use these records to run the program and grant Rewards, to stop the same invitation from being rewarded more than once, and to monitor, audit, and investigate invitations, sign-ups, and Rewards for fraud and abuse, including by linking and reviewing the accounts involved, as described in Section 2.2.2 and in Section 9.2 of the Terms. The person who invited you may be told that an account joined or qualified through their invite.

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.
- Advertising partners, which may indicate to us that a visit or an action began with one of their ads or promoted links, including by attaching an identifier to the link you followed to reach the Service (see Section 10.1).
- 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 may use the information we collect for any or all of the following purposes, among others:

- Operating the Service, authenticating users, and resolving turns.
- Building, training, fine-tuning, evaluating, benchmarking, distilling, red-teaming, and otherwise improving AI systems, models, agents, datasets, and tools — including the Resolver, future Resolvers, successor products, spin-off and unrelated games and products, and research models, whether developed by us or by our current or future vendors, partners, licensees, affiliates, acquirers, or successors — and including work on their general intelligence and reasoning, physics and world simulation, storytelling and narrative generation, dialogue and character behavior, agent planning and tool use, image curation, selection, captioning, and generation, audio and video generation, voice and speech, moderation and safety systems, evaluation benchmarks and test sets, and any other capability of such systems.
- 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, or object as described in Section 7.1.

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 to use, access, process, analyze, index, combine, enrich, aggregate, de-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 the purposes described in Section 3 and for any other purpose materially similar to, or a natural extension of, those purposes, including the development, training, evaluation, and commercialization of AI systems, models, datasets, tools, and products of any kind, whether or not related to the Service, and the creation and operation of new, spin-off, successor, and unrelated products and lines of business. Where a legal basis is required for this processing under applicable data protection law, we rely on the bases described in Section 7.1, principally our legitimate interests, and not on your consent; this Section is a grant of rights and is not itself the legal basis for that processing.

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.

De-identified and aggregated data. Where we de-identify or aggregate information so that it can no longer reasonably be linked to you or to your household or device, that information is no longer personal information, and we may use, disclose, license, sell, and otherwise exploit it for any purpose without restriction, including for the purposes in Sections 3 and 3.1. We maintain and use such de-identified data only in de-identified form, take reasonable measures to ensure that it cannot be associated with an individual, publicly commit not to attempt to re-identify it except to test whether our de-identification is effective where the law permits, and contractually require any recipient of it to comply with the same commitments.

4. How We Share Information

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

- Service providers and sub-processors, including cloud hosting, storage, compute, content delivery, analytics, telemetry, email delivery, push notification and messaging, payment processing and tax determination, anti-fraud, identity and age verification, advertising and marketing measurement, and customer support vendors. We may add, change, or remove such providers at any time.
- Advertising partners, meaning the platforms, networks, and services on which we advertise or promote the Service, which may receive the information described in Section 10.1, including information sent from our servers. Except where a partner has agreed to act only on our behalf, it uses that information for its own purposes and under its own terms, including to measure and improve advertising, to build audiences, and to show advertising to you and to others on its own and other services.
- 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.
- Anyone who opens an invite link or code you share, who may see your display name as the person who invited them.
- Affiliates and corporate successors, including in connection with a merger, acquisition, reorganization, financing, bankruptcy, or sale of the Service, of the business, or of any of its assets, and prospective parties to such a transaction during due diligence. Your information — including the AI training corpus and every dataset, model, and derived artifact created from it — is a transferable asset of the business, and a purchaser or successor may continue to use it as this Policy describes.

- AI developers, research partners, and licensees, purchasers, and other recipients of datasets, models, and derived data products that we create from the information described in Section 3.1, who may receive that information — including in identifiable form where the license or sale so provides — for their own purposes and under their own terms.
- 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. Disclosures to advertising partners described in Section 10.1 may be treated as a “sale” or “sharing” of personal information, or as “targeted advertising,” under some laws; Sections 7.2 and 10.2 describe how to opt out. 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. Because those purposes differ, we determine the period for each category by reference to criteria rather than a single fixed term. The criteria we apply are: the life of your account and of the world your character plays in; our operational, continuity, security, and abuse-prevention needs; our need to develop, train, evaluate, and improve AI systems, for which gameplay content, agent instructions, Resolver outputs, generated media, and the underlying AI request and response records are kept for as long as they remain useful for those purposes; the periods required by tax, accounting, and anti-fraud law; the periods needed to establish, exercise, or defend legal claims; and the periods needed to enforce bans and the character-limit and multiple-account rules in Section 4.2 of the Terms. Records held for safety, security, abuse prevention, or ban enforcement may be kept after an account is closed or terminated, for as long as those criteria require.

Identifiers that an advertising partner attaches to a visit (such as a click identifier carried in the address of the link you followed) are held by us only for as long as needed to determine whether that visit led to an action we report under Section 10.1, and are then deleted. Once a report has been sent, we may hold nothing that connects you or your account to it. Identifiers that a partner’s own technology stores in your browser or device last for the period that partner sets, and information a partner has received is retained under its own policies.

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, and we do not guarantee the security of your information. You acknowledge that your use of the Service carries a non-trivial risk that your information may be exposed, and you accept that risk. To the maximum extent permitted by applicable law, we exclude liability for any damages, losses, or harms resulting from any leak, hack, unauthorized access, or other security incident, regardless of cause, and where that liability cannot be excluded it is limited as set out in Section 13 of the Terms. Nothing in this Section excludes or limits liability that cannot be excluded or limited by law, including liability for intent or gross negligence, for death or personal injury caused by negligence, or any remedy available to you under applicable data protection law.

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. 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, to prevent fraud and abuse, and to develop, train, evaluate, and improve AI systems as described in Sections 3 and 3.1); consent (for certain marketing and tracking, where consent is required); and compliance with legal obligations. Where we rely on legitimate interests you may object to that processing, including our use of your content to develop and train AI systems, by using any control we provide in your account settings or by writing to contact@elusive10.com. An objection takes effect for the future: we will stop including your content in AI development from that point, and it does not require us to unpick material already used, already combined with other users' content, or already incorporated into a trained model. 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” of personal information or “targeted advertising”), and to limit the use of “sensitive

personal information,” subject to exceptions. We will not discriminate against you for exercising these rights.

Disclosures we make to advertising partners (Section 10.1) may be treated as a “sale” or “sharing” of personal information, or as “targeted advertising,” under some state laws. You can opt out of them in the ways described in Section 10.2. In particular, if your browser or a browser extension sends a Global Privacy Control signal, we treat it as a valid request to opt out of the sale or sharing of your personal information and of targeted advertising: we act on it automatically, without an account, without any further step on your part, and without changing your experience of the Service. You can turn the signal on in a browser that supports it or by installing an extension that sends it. You may also submit an opt-out request by emailing contact@elusive10.com. For visitors in states with such laws, we may also ask an advertising partner to treat what we send it as our service provider or processor — that is, to use it only on our behalf and not for its own advertising. We do not knowingly sell or share the personal information of anyone under 18, because the Service is not open to them (Section 11).

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.

7.4 Israel

The Service is operated from Israel, and this Policy also serves as the notice required by Section 11 of the Protection of Privacy Law, 5741-1981. You are under no legal duty to provide us with any information; providing it depends on your free will, but without the information described in Section 2.1 we cannot provide the Service. The purposes for which information is requested and the persons to whom it may be delivered are described in Sections 3 and 4. You have rights of access and correction under Sections 13 and 14 of that law, exercisable by writing to contact@elusive10.com, and you may apply to the Privacy Protection Authority.

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 and any other country in which we, our service providers, or our advertising partners operate, and those countries may have data protection laws that are different from, and less protective than, those of your country. Where such a transfer is subject to the GDPR or the UK GDPR, we rely on an adequacy decision where one applies and otherwise on the European Commission’s standard contractual clauses, with the UK addendum where relevant, as included in our providers’ data processing terms; a copy of the relevant safeguards is available on request to contact@elusive10.com.

Where permitted, we may also rely on another lawful transfer mechanism, including a derogation for specific situations under applicable law.

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 may 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. In all other cases, automated decisions are final.

10. Cookies and Similar Technologies

We, our service providers, and our advertising partners may use cookies, local storage, SDKs, pixels, tags and scripts, device and browser identifiers, identifiers carried in web addresses (for example, a click identifier that an advertising platform adds to a link you follow to reach the Service), reports sent from our servers to a partner's servers, and similar technologies — whether they operate in your browser or device or on our servers — to authenticate users, remember preferences, measure performance, conduct analytics, and (where lawful) support advertising, including its measurement, attribution, optimization, and targeting, as Section 10.1 describes. Where the law requires consent for such a technology, we will obtain it, through a consent management tool or another appropriate mechanism, at the time that technology is used. You can also manage cookies through your browser settings; disabling certain cookies may impair the Service.

10.1 Advertising

We may advertise and promote the Service on third-party platforms and services — such as social networks and online communities, search engines, AI assistants, chatbots, and other conversational or generative AI services, video and streaming services, messaging services, app stores, games and gaming platforms, and advertising networks — and we may use their technologies and our own to measure, attribute, optimize, and improve that advertising and the audiences it reaches. This may include learning whether an ad or a promoted link led to a visit, an account registration, the creation of a character, a purchase or subscription, or another action in the Service. Whether, where, and for whom any of this is used may vary by partner, page, location, and time, and we may add, change, or remove advertising partners at any time. This Section does not apply to Google User Data, which is governed by Section 14.

Information may reach an advertising partner in more than one way, including the following. A partner's technology placed on a page of the Service (such as a tag, script, pixel, or cookie) may send information directly from your browser or device. Separately, our own servers may send information to a partner — for example, to report that a visit which began with one of its

ads went on to an action in the Service — including where no partner technology is present in your browser and no cookie is set.

The information involved may include: an identifier that the partner attached to the link that brought you to the Service, or that its technology stored in your browser or device; the fact, type, and time of an action in the Service and, for a purchase, its amount and currency; a random or hashed reference for the event or for your account; your IP address and the approximate location derived from it; browser, device, and screen information; the address of the page you visited and of the page that referred you; and cookie and other online identifiers. A partner may be able to link what it receives to an account you hold with it, and may combine it with other information it holds and with information about your activities over time and across other websites, apps, and services.

Except where a partner has agreed to act only on our behalf, each partner determines its own uses of that information under its own terms and privacy policy, which we do not control and for which we are not responsible. Those uses may include measuring and reporting on our advertising; developing, improving, and optimizing its own products, services, and advertising systems; building audiences of people who have visited the Service or taken an action in it, and of people with similar characteristics; and showing advertising — ours or others' — to you and to such audiences on the partner's own services and elsewhere.

Where a partner offers a way to do so, we may mark the information we send it with an instruction — for example, that the partner should not use it to personalize advertising to you, or should use it only on our behalf. Whether and how a partner acts on such an instruction is determined by that partner under its own terms, and we make no representation about it.

We may limit these practices by location. Where the law of the place you are in requires your prior consent for a technology or disclosure described in this Section, Section 10 applies and we will not use it without that consent. We may publish within the Service a list of the advertising partners we currently work with; where we do, it forms part of this Section and may change at any time without a change to this Policy.

10.2 Your Advertising Choices

You can limit or opt out of the practices described in Section 10.1 in any of the following ways, and you may use more than one of them.

- **Global Privacy Control.** If your browser or a browser extension sends a Global Privacy Control signal, we treat it as a request to opt out of the sale or sharing of your personal information and of targeted advertising, to the extent those terms apply to us, and in particular we will not send a partner the server-side reports described in Section 10.1 for a visit that carries the signal. We do this automatically, with no account and no further step required, and without changing your experience of the Service.

- Browser and device controls. You can block or delete cookies and other site data through your browser settings, and limit tracking through the privacy settings of your browser or device. Doing so may impair the Service.
- Partner settings. You may be able to limit how an advertising partner uses information about you, including for personalized advertising, through the advertising or privacy settings that partner offers in your account with it or on your device.
- Contacting us. You may ask us to opt you out of the sale or sharing of your personal information and of targeted advertising by emailing contact@elusive10.com. Because we may hold nothing that links you to a report already sent to a partner (Section 5), we may be able to act only for the future, and anything a partner already holds is subject to that partner's own process, to which we may refer you.

Opting out does not stop you from seeing advertising; it affects how information about your use of the Service is used for advertising. The Service does not respond to browser "Do Not Track" signals, except where applicable law requires otherwise.

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 and we will take appropriate steps to delete it and terminate the account.

12. Marketing Communications

We may send you service, transactional, and marketing messages about the Service and related offerings, by email, push notification, in-Service message, or any other channel we may offer from time to time. You can opt out of marketing messages by following the unsubscribe instructions in the message, adjusting your notification settings, or withdrawing the permission your browser or device gave us. 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.

For clarity, a report to an advertising partner under Section 10.1 that an action occurred in the Service (for example, that an account was registered after a visit that began with an ad) does not involve Google User Data and is not a transfer of it, provided the report contains none of the information described in Section 14.1.

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 character-limit 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. We keep it for as long as those purposes require and no longer, we use it only for those reasons while we keep it, and we handle it in accordance with the Google API Services User Data Policy. 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 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

Avasta is operated by Evyatar Or, an individual who operates the Service personally as a registered dealer (עוסק מורשה) in Israel and not through a company, and who is the controller of the personal information described in this Policy. Questions, complaints, or rights requests can be sent to contact@elusive10.com, or by mail to Avasta, P.O. Box 18049, Tel Aviv-Jaffa HaHashmonaim St 88 zip code 6713305, Israel. Our representative in the European Union, designated under Article 27 of the GDPR, is Rickert Rechtsanwaltsgesellschaft mbH, – elusive10 / Avasta –, Colmantstraße 15, 53115 Bonn, Germany (art-27-rep-elusive10@rickert.law). Our representative in the United Kingdom, designated under Article 27 of the UK GDPR, is Rickert Services UK Ltd, – elusive10 / Avasta –, PO Box 1487, Peterborough PE1 9XX, United Kingdom (art-27-rep-elusive10@rickert-services.uk). You may contact either of them, in addition to or instead of us, on any matter relating to our processing of your personal data.