Astrala Advisory Services Ltd — Privacy Policy

Effective Date: March 2026
Version: 1.0
Reviewed by: Director / Data Protection Lead
Next review due: March 2027

---

1. Who We Are

Astrala Advisory Services Ltd is a private limited company registered in Cyprus under the Cyprus Companies Law (Cap. 113), with registered company number HE 480652 and registered office in Nicosia, Cyprus.

Astrala Advisory Services Ltd ("Astrala", "we", "us", "our") is an operations and technology partner for international professional services firms, providing three core service lines:

- Financial Operations Shared Services (BPO): end-to-end payroll processing (multi-currency, multi-jurisdiction), credit control and debtor management, management accounts preparation, and compliance support.
- IT Infrastructure & Operations Outsourcing: management of cloud-based accounting and CRM tools, IT security, access management, and licence optimisation for affiliated group companies and external clients.
- Astrala Nexus AI Talent & Competence Platform (SaaS): AI-driven candidate matching using skills and emotional-intelligence profiling, recruitment coordination, and workforce development tools.

We serve clients primarily in the UK, EU, MENA, and India, operating from our Cyprus base.

For the purposes of data protection law, Astrala Advisory Services Ltd acts as:

- Data Controller — where we determine the purposes and means of processing personal data, including for the operation of the Astrala Nexus platform, our own marketing and business development, our internal HR and employment activities, and service delivery where we have independent discretion over how personal data is used.
- Data Processor — where we process personal data on behalf of, and strictly on the documented instructions of, our clients (for example, when processing client employee payroll data or managing client IT systems under a Managed Operational Support agreement).

Where Astrala acts as a processor, the client remains the data controller and is responsible for their own compliance obligations. In those cases, Astrala processes personal data only as described in the applicable Data Processing Agreement (DPA) and Scope of Work agreement.

2. Legal Framework

Astrala Advisory Services Ltd is committed to protecting personal data in compliance with:

- Regulation (EU) 2016/679 (EU General Data Protection Regulation — "EU GDPR"), which applies directly in Cyprus as an EU Member State;
- The Law Providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of Such Data, Law No. 125(I)/2018 (Cyprus Data Protection Act), which supplements the EU GDPR with Cyprus-specific provisions;
- The Regulation of Electronic Communications and Postal Services Law (Law 112(I) of 2004, as amended) in respect of electronic marketing and cookies.

The supervisory authority in Cyprus for EU GDPR purposes is the Commissioner for the Protection of Personal Data, located at 15 Kypranoros Street, 1061 Nicosia, Cyprus.

Where Astrala processes the personal data of UK-based individuals and is subject to UK GDPR (for example, in connection with services delivered to UK clients or through the Astrala Nexus platform used in the UK), Astrala complies with the UK GDPR and the Data Protection Act 2018 in addition to EU GDPR requirements. The relevant UK supervisory authority is the Information Commissioner's Office (ICO).

---

3. What Personal Data We Collect

Astrala collects and processes personal data across its three service lines and internal operations. The categories depend on the service context:

3.1 Astrala Nexus Platform (Candidates and Employer Representatives)

For candidates and hiring managers using the Astrala Nexus platform:

- Identity and Contact Data: name, email address, telephone number, job title, company name, and account credentials.
- Profile and CV Data: employment history, education, qualifications, skills, certifications, job preferences, uploaded CV documents, and content of in-platform messages.
- Psychometric, EQ, and Assessment Data: results of personality assessments (including OCEAN framework scores), emotional intelligence (EQ) ratings, soft-skill evaluations, wellbeing indicators, and AI-generated conversational insights produced by the Clara AI engine. This data is treated as sensitive personal data and processed with explicit consent or under another valid legal basis.
- Symbolic Profiling Data (MVP3 onwards): archetype classifications, factor scores (openness, conscientiousness, extraversion, agreeableness, neuroticism, and derived factors), mood board states, and the Been/Being/Becoming developmental profile. This evolving profile is

linked to the candidate's platform account and updated dynamically as they engage with the platform.

- Diversity and Sensitive Data: where you voluntarily provide it, data about ethnicity, gender, disability status, or other demographic information for diversity monitoring purposes. Provision of such data is entirely optional and processed only with explicit consent or under a specific lawful basis (e.g. equality legislation compliance). It is typically used only in anonymised or aggregated form.
- Identity Verification Data: copies of identification documents (e.g. passports, driving licences, right-to-work documents) where required to verify a candidate's eligibility.
- Usage and Technical Data: IP address, device and browser type, session data, feature usage, and interaction logs, collected automatically via platform analytics tools (PostHog).
- Communication Data: messages and correspondence sent through the platform, including Clara AI conversation logs, manager feedback, and support communications.
- Payment and Transaction Data (Employer clients): billing name, company, billing address, and transaction confirmation details. Full payment card numbers are never stored by Astrala; payments are processed via a secure third-party payment processor (e.g. Stripe).

Job seeker profiles on Astrala Nexus are private by default. Profile information and CVs are not visible to any employer unless the candidate actively applies to a role or explicitly shares their profile. Employers cannot access candidate profiles without the candidate's active consent.

3.2 Financial Operations & IT Services (Client Employees and Contacts)

When delivering payroll, credit control, accounts, and IT managed services to clients:

- Employee and Payroll Data: names, employee numbers, national identification numbers, salary information, bank account details, tax codes, pension contributions, social insurance numbers, payroll history, and employment status — processed strictly on behalf of and on the instructions of the client (who is the data controller of this information).
- Financial and Accounting Data: debtor and creditor information, invoices, payment records, management account data, and financial transaction history — processed on behalf of the client.
- IT and Access Management Data: user account credentials, system access logs, device identifiers, software licence assignments, and IT support tickets — processed on behalf of the client.
- Client Contact Data: names, email addresses, telephone numbers, and job titles of client personnel and their counterparties, used to deliver and communicate about our services.

3.3 Internal Operations (Staff, Contractors, Candidates for Employment)

For our own team members, contractors, and job applicants:

- Employment Data: name, contact details, right-to-work documentation, employment contracts, salary, pension, performance records, and training records.
- Recruitment Data: CVs, application forms, interview notes, and reference checks for candidates applying to work at Astrala.

3.4 Research Data (Anonymised — Astrala Nexus Research Layer)

The Astrala Nexus platform includes a dedicated research layer for diversity, inclusion, and workforce analytics research. This layer operates strictly on anonymised data only. No personally identifiable information (PII) is ever written to the research schema. Personal identities, emails, and platform IDs are stripped by an automated anonymiser before any data enters the research tables. Access to research data is restricted to authorised researcher roles only, enforced by database-level Row-Level Security policies.

---

4. How We Use Personal Data

4.1 Astrala Nexus Platform

- Platform operation and account management: creating and maintaining user accounts, enabling job matching and application workflows, facilitating candidate–employer connections, and providing the Clara AI co-pilot assistant.
- AI-powered matching and recommendations: using candidate profiles (including EQ scores, factor profiles, and skills data) to generate ranked shortlists and match recommendations for employers. No final hiring decision is made solely by automated means — human review and approval are always required before decisions are communicated.
- Automated manager communications: sending shortlist summaries, interview scheduling proposals, nudge messages, and campaign performance updates on behalf of Astrala's recruitment clients, as part of the Clara Nexus MVP 2.0 recruiter co-pilot function.
- Onboarding and aftercare journeys: triggering welcome sequences, 30/60/90-day check-ins, and early-risk flagging for placed candidates, to support retention for employer clients.
- Platform improvement and analytics: analysing aggregated usage patterns, feature adoption, and platform performance using PostHog analytics and Sentry error monitoring, to improve and secure the platform.
- Security and fraud prevention: detecting unauthorised access, misuse, and security incidents; verifying user identities where appropriate.
- Marketing (with consent): sending newsletters and promotional communications about platform features or services only where you have opted in. You may withdraw consent at any time via the unsubscribe link in any marketing email.
- Research (anonymised only): contributing anonymised, non-identifiable interaction data to the platform's research layer, subject to explicit consent at onboarding, to support diversity and workforce development research.

4.2 Financial Operations and IT Services

- Processing payroll, managing debtor collections, preparing management accounts, and providing IT support and infrastructure management — all on behalf of and under the instructions of our clients (acting as data processor).
- Communicating with client personnel and their counterparties as necessary to deliver contracted services.
- Maintaining records required for legal and regulatory compliance (e.g. tax, accounting, employment law obligations).

4.3 Internal Operations

- Recruiting, onboarding, and managing Astrala employees and contractors in compliance with Cyprus employment law.
- Administering payroll, pension, and benefits for Astrala's own staff.
- Meeting Astrala's own legal and regulatory obligations as a Cyprus company.

---

5. Legal Bases for Processing

Under EU GDPR Article 6, Astrala relies on the following legal bases:

Processing Activity	Legal Basis
Operating Astrala Nexus accounts and delivering SaaS services	Performance of a contract (Art. 6(1)(b))
Delivering BPO/IT services under client agreements	Performance of a contract / Legitimate interests (Art. 6(1)(b)/(f))
AI matching, shortlisting, campaign automation, onboarding journeys	Performance of a contract (Art. 6(1)(b))
Internal HR, employment, and payroll	Legal obligation + contract (Art. 6(1)(b)/(c))
Platform security, fraud prevention, analytics	Legitimate interests (Art. 6(1)(f))
Marketing communications	Consent (Art. 6(1)(a))
Optional diversity data	Explicit consent (Art. 9(2)(a))
Psychometric / EQ / symbolic profile data	Explicit consent (Art. 9(2)(a)) + contract (Art. 6(1)(b))
Research layer (anonymised data only)	Explicit consent (Art. 6(1)(a)) / Legitimate interests
Compliance with tax, audit, and legal obligations	Legal obligation (Art. 6(1)(c))

Where Astrala relies on legitimate interests, these have been assessed against data subjects' rights and freedoms. You have the right to object to processing based on legitimate interests (see Section 9).

Where Astrala relies on consent, you may withdraw consent at any time without affecting the lawfulness of any processing carried out before withdrawal.

---

6. Special Category Data

Certain categories of personal data require heightened protection under EU GDPR Article 9, including psychometric and personality assessment data, health and wellbeing data, and diversity data (ethnicity, disability status, gender).

Astrala processes such data only where:

- Explicit consent has been given (e.g. OCEAN profiling, diversity monitoring, wellbeing monitoring via Clara EQ);
- Processing is necessary for employment law obligations (e.g. reasonable adjustments for disability);
- Processing is necessary for equality legislation compliance in connection with the services Astrala delivers to clients.

Under Cyprus Law No. 125(I)/2018, processing of genetic and biometric data for life and health insurance purposes is prohibited, and any further processing of genetic or biometric data beyond its original consent purpose requires a separate, specific consent.

Data subjects retain the right to withdraw consent to special category processing at any time. Withdrawal of consent to EQ/psychometric profiling will disable personalised AI matching features on the Astrala Nexus platform; the account will remain functional with standard (non-profiled) matching.

---

7. Automated Decision-Making and Profiling

The Astrala Nexus platform uses automated profiling to compute match scores, rank candidates, generate shortlists, and personalise the Clara AI assistant's responses. This profiling draws on OCEAN personality scores, derived factor scores, EQ assessments, and historical platform interactions.

No hiring decision or career outcome is made solely by automated means without human review. Recruiters and hiring managers review, approve, or adjust all AI-generated shortlists and recommendations before they are communicated to candidates or clients. This approach is consistent with EU GDPR Article 22.

Data subjects have the right to:

- Request human review of any significant decision involving automated profiling;
- Express their point of view;
- Contest an automated decision.

To exercise this right, contact us at the details in Section 11.

---

8. Sharing of Personal Data

8.1 Sharing with Employers (Astrala Nexus — Candidates)

Where a candidate applies for a role or explicitly shares their profile with an employer through Astrala Nexus, relevant personal data (e.g. name, CV, match scores, application responses) is transmitted to the employer. Upon receipt, that employer becomes an independent data controller of the candidate's personal data and is responsible for its subsequent use. Astrala contractually requires employers to use candidate data only for recruitment purposes.

8.2 Sharing with affiliated group companies and Client Companies

Personal data processed under BPO and IT services agreements is shared within the affiliated group companies and with relevant third parties strictly to the extent required to fulfil contracted services and on documented client instructions.

8.3 Service Providers (Processors)

Astrala engages trusted third-party service providers who process personal data on our behalf. All such providers are subject to written data processing agreements and are authorised to process data only for the purposes specified by Astrala. Key categories include:

Provider Category	Example / Tool	Purpose
Cloud hosting & database	Supabase Cloud, Vercel	Platform hosting, data storage
AI / Conversational AI	Anthropic Claude API	Clara AI response generation
Emotional Intelligence AI	Pi (Inflection AI)	EQ scoring, tone calibration, wellbeing detection
HRM Integration	Sapient HRM API	Job sync, candidate push, placement tracking
Product analytics	PostHog	Usage analytics, feature flags
Error monitoring	Sentry	Platform error tracking and performance
Payment processing	Stripe (or equivalent)	Subscription billing for employer clients
Email and communications	[Designated provider]	Transactional and marketing email delivery
Accounting software	Xero / MS 365	Financial operations for clients

8.4 Legal Disclosures

Astrala may disclose personal data to public authorities, law enforcement, or regulators where required to do so by law, court order, or applicable regulation, or where necessary to protect the rights, property, or safety of Astrala, its clients, or third parties.

Astrala does not sell personal data to third parties. Astrala does not share personal data with third parties for their own direct marketing purposes.

---

9. International Data Transfers

Astrala Advisory Services Ltd is established in Cyprus (EU/EEA) and operates as an EU data controller. Personal data processed by Astrala may be transferred outside the EU/EEA in the following circumstances:

- To the United Kingdom: The EU Commission has recognised the UK as providing an adequate level of data protection under Article 45 EU GDPR (adequacy decision). Transfers to UK-based clients and processors are made on this basis.
- To MENA and India (operational scope): As Astrala develops its service presence in MENA and India, personal data transfers to these jurisdictions will be made subject to appropriate safeguards under EU GDPR Article 46, including Standard Contractual Clauses (SCCs) approved by the European Commission, supplemented by transfer impact assessments where required.
- To Andorra (Clara Futura SL): As a co-investor and related party in the Clara Nexus platform, Clara Futura SL (registered in Andorra) may receive relevant platform data. Andorra is recognised as providing adequate protection under EU GDPR; transfers are conducted under appropriate contractual arrangements.
- Cloud Service Providers: Astrala prioritises EU/EEA data residency for its cloud infrastructure. Where data is processed by providers (e.g. Anthropic, Inflection AI) in countries outside the EU/EEA, Astrala ensures appropriate SCCs or equivalent safeguards are in place.

Under Cyprus Law No. 125(I)/2018, prior notification to the Commissioner is required before transferring sensitive (special category) personal data to a third country not covered by an EU adequacy decision.

---

10. Data Retention

Astrala retains personal data only for as long as is necessary for the purposes for which it was collected, taking into account applicable legal, tax, and regulatory retention requirements.

Data Category	Retention Period
Astrala Nexus candidate profiles (active)	Duration of account + 2 years after last activity, or until deletion requested

Astrala Nexus candidate profiles (inactive/unmatched)	12 months from last login, then pseudonymised or deleted
Payroll and financial records (client BPO)	7 years from the end of the relevant financial year (Cyprus/UK tax law requirements)
Employment records (Astrala staff)	Duration of employment + 6 years
Management accounts and audit records	7 years
IT system access logs	12 months
Clara AI conversation logs	12 months from last session, or account deletion, whichever is earlier
Research schema data (anonymised)	Indefinite (as no PII is held); tied to research project lifecycle
Marketing consent records	Duration of consent + 3 years

When personal data is no longer required, it is securely deleted or anonymised. Where deletion is not immediately possible (e.g. backup media), data is isolated and protected from further processing until deletion is completed.

---

11. Your Rights as a Data Subject

Under the EU GDPR and Cyprus Data Protection Act, you have the following rights in relation to your personal data:

- Right of Access (Art. 15): the right to obtain confirmation of whether we process your personal data and to receive a copy of it, together with information about how it is processed.
- Right to Rectification (Art. 16): the right to have inaccurate personal data corrected and incomplete data completed.
- Right to Erasure / "Right to be Forgotten" (Art. 17): the right to request deletion of your personal data where it is no longer necessary, consent has been withdrawn, or processing was unlawful — subject to legal retention obligations.
- Right to Restriction of Processing (Art. 18): the right to request that we restrict the processing of your personal data in certain circumstances (e.g. while accuracy is contested).
- Right to Data Portability (Art. 20): the right to receive personal data you have provided to us in a structured, commonly used, machine-readable format, and to transmit it to another controller, where processing is based on consent or contract and carried out by automated means.
- Right to Object (Art. 21): the right to object to processing based on legitimate interests, and the right to object to processing for direct marketing purposes at any time.

- Rights in Relation to Automated Decision-Making (Art. 22): the right not to be subject to a decision based solely on automated processing that produces significant legal or similarly significant effects — and the right to request human review, to express your view, and to contest the decision.
- Right to Withdraw Consent: where processing is based on consent, the right to withdraw that consent at any time, without affecting the lawfulness of prior processing.

To exercise any of these rights, contact us using the details in Section 13. We will respond within one calendar month of receiving your request (or within three months for complex or numerous requests, with notice of the extension given within the first month).

We will not charge a fee for legitimate requests. However, where requests are manifestly unfounded, excessive, or repetitive, a reasonable administrative fee may be charged or the request refused, with reasons given.

---

12. Security

Astrala implements appropriate technical and organisational measures to protect personal data against unauthorised access, accidental loss, destruction, or alteration. Measures in place include:

- Database-level Row-Level Security (RLS) on all Astrala Nexus platform tables, enforced by Supabase PostgreSQL — users access only their own data; admin roles cannot bypass the research schema.
- Role-based access controls with four roles (candidate, manager, admin, researcher), each with strictly scoped data access.
- Encrypted data in transit (TLS/HTTPS) for all platform and API communications.
- Supabase Auth with email/OAuth authentication and support for enterprise SSO (SAML 2.0, OIDC) for enterprise clients.
- API key and secret management via environment variables — never exposed in client-side code.
- Error monitoring and alerting via Sentry for real-time incident detection.
- Anonymised research data — no PII ever enters the research schema; the anonymiser processes all data before insertion.
- Regular security reviews including GDPR/compliance audits at each major development milestone.

In the event of a personal data breach that is likely to result in a risk to data subjects' rights and freedoms, Astrala will notify the Commissioner for the Protection of Personal Data within 72 hours of becoming aware of the breach (EU GDPR Art. 33), and will notify affected data subjects without undue delay where the breach is likely to result in a high risk (EU GDPR Art. 34).

---

13. Cookies and Tracking Technologies

The Astrala Nexus platform uses cookies and similar tracking technologies to provide platform functionality, measure performance, and improve the user experience. A dedicated Cookies Policy describes the specific cookies used, their purpose, and how to manage preferences. Where non-essential cookies are used, consent is obtained before placement.

The platform uses PostHog for product analytics and feature flags, and Sentry for error monitoring — both of which may process limited technical data (e.g. anonymised session data, error logs).

---

14. Data Protection Officer

Astrala Advisory Services Ltd has designated a Data Protection Lead responsible for overseeing compliance with EU GDPR and Cyprus data protection law. Contact details are provided in Section 13 below.

Astrala will keep under review whether formal appointment of a Data Protection Officer (DPO) is required as the business scales, in accordance with EU GDPR Article 37 and the Cyprus Data Protection Act (Section 14, Law No. 125(I)/2018). The Commissioner may publish a list of cases requiring DPO appointment.

---

15. Children's Data

The Astrala Nexus platform is not directed at children and does not knowingly collect personal data from individuals under the age of 14 years. Under Cyprus Law No. 125(I)/2018, the minimum age for a child to independently consent to information society services is 14 years (lower than the GDPR default of 16).

Where a user under 14 is identified, their account will be suspended and their data deleted unless verifiable parental or guardian consent is provided.

---

16. Changes to This Policy

Astrala may update this Privacy Policy from time to time to reflect changes in its services, legal requirements, or operational circumstances. Where significant changes are made, Astrala will notify data subjects by appropriate means — for example, by email notification or a prominent notice within the Astrala Nexus platform. The "Effective Date" at the top of this policy indicates when the current version took effect.

Data subjects are encouraged to review this policy periodically. Continued use of Astrala's services following notification of updates constitutes acknowledgment of the revised policy.

---

17. Contact Us

For any questions, concerns, or requests regarding this Privacy Policy or the exercise of your data protection rights, please contact:

Data Controller:
Astrala Advisory Services Ltd
Registered in Cyprus, Company No. HE 480652
Registered Office:

Data Protection Lead:
Email: privacy@astralaadvisory.com (update with confirmed address)
General enquiries: hello@astralaadvisory.com (update with confirmed address)

If you believe your data protection rights have not been adequately addressed, you have the right to lodge a complaint with the Commissioner for the Protection of Personal Data (Cyprus supervisory authority):

Commissioner for the Protection of Personal Data
15 Kypranoros Street
1061 Nicosia, Cyprus
Website: www.dataprotection.gov.cy

If you are based in the UK and your complaint relates to the processing of your personal data under UK GDPR, you may also contact the Information Commissioner's Office (ICO) at www.ico.org.uk.

Astrala welcomes the opportunity to address privacy concerns directly and is committed to resolving any data protection issues promptly and to the satisfaction of all parties.

This Privacy Policy is issued by Astrala Advisory Services Ltd and is intended for use across all Astrala Advisory services, including the Astrala Nexus platform, financial operations shared services, and IT infrastructure outsourcing. It supersedes any prior privacy notices issued by Astrala Advisory Services Ltd.