Privacy Policy

Privacy notice for the Trendi Platform Ecosystem

Trust is protected through responsible data use.

Document	Trendi Global Privacy Policy
Version	01Jun26_V4.1
Effective date	01 June 2026
Publication location	Trust, Privacy & Governance
Applies to	Website visitors, Clients, Client Administrators, End Clients, Partners, employees, applicants, candidates, scholars, learners, bursary applicants, Developers, Marketplace Participants and other Trendi ecosystem participants.

Document navigator

This Policy is the privacy-specific document in the Trendi legal stack. It should be read with the Trendi Global Platform Terms and Conditions and any workflow-specific privacy notice in the portal.

Part	Focus
PART A - PRIVACY FOUNDATION	Scope, contact details, privacy roles and who this Policy covers.
PART B - PERSONAL INFORMATION AND LAWFUL USE	Information categories, sensitive information, collection methods, purposes and lawful bases.
PART C - AI, ANALYTICS, SHARING AND TRANSFERS	AI Services, Platform Data, de-identified insights, disclosures and international transfers.
PART D - SECURITY, RETENTION, RIGHTS AND UPDATES	Security, incidents, retention, cookies, marketing, privacy rights, complaints and updates.
ANNEXURES	Practical data map and purposes / safeguards reference.

PART A - PRIVACY FOUNDATION

Applies across the Trendi Global platform ecosystem and explains how this Policy works with the wider legal stack.

1. Purpose, scope and relationship with the Platform Terms and Conditions

This Privacy Policy explains how Trendi collects, uses, shares, stores, protects and governs Personal Information across the Trendi Global platform ecosystem. It is designed to sit alongside the Trendi Global Platform Terms and Conditions without repeating the commercial, intellectual property, payment, step-in, developer, marketplace or broader platform governance terms contained in those Terms.

This Policy applies to Personal Information processed by or through the Platform, including websites, portals, workspaces, applications, APIs, integrations, support channels, applicant journeys, assessment workflows, #MyCareer workflows, AI Services, Digital Workers, marketplace functionality, developer environments, client workspaces, partner workspaces and related operational services.

This Policy should be read together with the Trendi Global Platform Terms and Conditions, any applicable Trendi Client Platform Subscription Agreement, the PAIA Manual, relevant Commercial Documents and any workflow-specific privacy notice. Capitalised words used in this Policy have the same meaning as in the Platform Terms and Conditions unless this Policy defines them differently.

If there is an inconsistency between this Policy and the Platform Terms and Conditions about the processing of Personal Information, the interpretation that gives better effect to applicable privacy law will apply. If there is an inconsistency about commercial, platform, intellectual property, payment, step-in, receivables or ecosystem governance matters, the Platform Terms and Conditions and the relevant Commercial Document will apply.

This Policy is a privacy notice. It does not create additional platform access rights, commercial rights, intellectual property rights, developer rights, marketplace rights or service-level commitments beyond those expressly stated in the Platform Terms and Conditions or a Commercial Document.

2. Who we are and how to contact us

For ease of use, this Policy refers to the platform ecosystem as “Trendi”, “Trendi Global”, “we”, “us” or “our”. Unless a Commercial Document identifies another authorised Trendi entity for a specific transaction, the default operational privacy contact and platform administration entity is Trending-Talent Solutions, Registration Number 2018/068302/07, acting as the Trendi Global Operations Centre (“TGOC”).

Current privacy, PAIA, information request, support and notice details may be published through the Trendi website, the Platform legal centre, the PAIA Manual, a Commercial Document, a data processing notice, a privacy notice presented during onboarding or another official Trendi channel.

Privacy contact	Details
Privacy / support	Website help icon or latest published Trendi privacy/support contact
Information Officer	Joe Pieterse
Deputy Information Officer	Mike Cross
PAIA Manual	Published on the Trendi website, Platform legal centre or made available on request
Office address	V&A Waterfront, Dock Road Junction, Cnr Stanley and Dock Road, Cape Town, 8001, South Africa

3. Privacy roles in the Trendi ecosystem

Privacy laws use different labels for similar roles. For purposes of this Policy, references to a "controller" include a responsible party where POPIA applies, and references to a "processor" include an operator where POPIA applies. Similar concepts under other laws should be interpreted consistently with the law that applies to the relevant processing.

Trendi may be a controller / responsible party for some processing activities and a processor / operator / service provider for others. The role depends on who determines the purpose and means of processing and the relevant Platform workflow, Commercial Document, Trendi Client Platform Subscription Agreement, Client instruction, Partner arrangement or Development Item.

Context	Typical privacy role
Direct Trendi accounts, website use, product analytics, security, support, billing and platform administration	Trendi usually acts as controller / responsible party for the relevant processing.
Client-controlled recruitment, employee, applicant, assessment, talent, learning or onboarding workflows	The Client or End Client may act as controller / responsible party and Trendi may act as processor / operator, unless the parties jointly determine purposes or another arrangement is documented.
Business Partner-led services for End Clients	The Business Partner and/or End Client may be responsible for client-side notices, lawful bases and service decisions. Trendi remains responsible for Platform processing it controls.
AI Services, Digital Workers, #MyCareer, platform analytics, fraud prevention, security and ecosystem governance	Trendi may act as controller / responsible party where it determines the platform purpose, safeguards, security and governance rules.
Marketplace or development items	Roles depend on the Development Item Registration, Marketplace listing, Commercial Document and who controls the data involved.

Where a Client, Business Partner, Partner Client or End Client provides Personal Information to Trendi or instructs Trendi to process Personal Information, that party must ensure that it has the required notices, lawful bases, consents, permissions, employment-law basis, programme basis, internal approvals and data subject communications in place. Trendi may refuse, restrict or suspend processing instructions that appear unlawful, unsafe, excessive, unclear, incompatible with this Policy, or inconsistent with the Platform Terms and Conditions.

4. Who this Policy applies to

This Policy applies to you where you interact with Trendi, use the Platform or participate in the ecosystem, including as:

- a visitor to a Trendi website, landing page, public page or legal centre;
- an Applicant User or participant in an application, assessment, learning, onboarding, verification, #MyCareer or career-related workflow;
- a Client User or Client Administrator;
- a Business Partner, Partner Client / End Client, partner employee or partner-appointed user;
- an Accredited Developer, Marketplace Participant, integration user or technical user;
- an Employee User of Trendi, a Client, a Business Partner, a Developer or another ecosystem participant;
- a supplier, service provider, support requester, payment participant, debtor contact or person who communicates with Trendi;
- an individual or juristic person whose information is submitted to or processed through the Platform, where applicable under privacy law.

PART B - PERSONAL INFORMATION AND LAWFUL USE

Explains what information may be processed and why Trendi may process it.

5. Personal Information we process

"Personal Information" in this Policy includes personal information under POPIA, personal data under GDPR or UK GDPR, and similar information under applicable privacy laws. It means information relating to an identified or identifiable natural person and, where applicable under POPIA, an identifiable existing juristic person.

The information we process depends on your role, the workspace, the Client or Partner instruction, the Platform workflow, applicable law and the relevant Commercial Document. We do not process every category for every person.

Category	Examples
Identity and contact	Name, surname, preferred name, identity or passport details where required, date of birth where relevant, email address, phone number, address and emergency or account contact details.
Account and access	Username, password metadata, workspace, role, permissions, administrator status, authentication logs, invitations, acceptance records and security settings.
Organisation and role	Company name, business unit, job title, department, partner status, developer status, accreditation status, reporting line, organisation registration and VAT information where relevant.
Applicant, career and assessment	CVs, qualifications, work history, skills, experience, applications, assessments, learning progress, career interests, work preferences, verification results and related workflow outputs.
Employment and talent workflow	Performance, development, engagement, retention, onboarding, training, succession, role fit, internal mobility and related talent-management information where authorised by a Client or Partner.
Platform and technical	IP address, device details, browser, cookies, logs, API usage, integration events, usage history, click patterns, page visits, system alerts, support diagnostics and audit records.
Billing and commercial	Invoices, billing records, payment status, account balances, purchase records, subscription records, Partner Revenue Participation records and receivables-related information.
Communications and support	Emails, support tickets, call notes, messages, feedback, surveys, training attendance, meeting notes and support interactions.
AI and automation data	Prompts, instructions, workflow inputs, AI outputs, Digital Worker activity, summaries, recommendations, classifications and human review records.

6. Special Personal Information, sensitive data and minors

Some Platform workflows may involve information that is treated as special, sensitive or regulated under applicable privacy law. This may include information relating to health, race or ethnicity, criminal background checks, biometrics, trade union membership, political or religious beliefs, employment matters, assessment data or other protected categories.

Trendi processes special or sensitive information only where it is lawful, relevant, necessary and authorised for the applicable workflow, and subject to appropriate safeguards. Where a Client, Partner or End Client asks Trendi to process such information, that party must ensure that it has the required lawful basis, notices, consents, authorisations and safeguards in place.

Where a workflow involves children or minors, Trendi will process Personal Information only where permitted by applicable law, such as with appropriate guardian or competent-person consent, Client or Partner authorisation, legal authorisation, programme requirements, or another lawful basis. Clients and Partners that submit information about children or minors must ensure that required permissions, notices and safeguards are in place.

7. How we collect Personal Information

We may collect Personal Information directly from you, from Clients or Partners, from authorised Users, from service providers, from third-party integrations, from public or permitted sources, and automatically through the Platform. This may occur when you:

- register, log in, accept an invitation, create an account or accept Platform documents;
- complete an application, assessment, profile, learning journey, onboarding workflow, #MyCareer workflow or other platform process;
- submit documents, credentials, CVs, qualifications, work history, verification information or support requests;
- use a Client workspace, Partner workspace, developer environment, API, integration or marketplace workflow;
- communicate with Trendi, attend training, respond to surveys, provide feedback or request support;
- use the website, cookies, analytics tools, AI Services, Digital Workers or other automated features;
- enter into or participate in a Commercial Document, Trendi Client Platform Subscription Agreement, billing process, payment flow, partner-client process or approved financing-related process.

Where we obtain Personal Information indirectly, the relevant Client, Partner, End Client or other source is responsible for providing required privacy notices unless Trendi is separately required by law to provide them.

8. Why we process Personal Information and lawful bases

We process Personal Information for the purposes below and for any additional purposes described in a specific privacy notice, Platform workflow, Commercial Document or Client / Partner instruction. We rely on one or more lawful bases recognised by applicable privacy laws, including consent where required, performance of a contract, compliance with legal obligations, legitimate interests, authorised Client or Partner instructions, protection of rights, and other lawful bases available in the relevant jurisdiction.

Purpose	Typical lawful basis / justification
Operate and provide the Platform	Contract performance, legitimate interests, authorised Client or Partner instructions, and consent where required.
Applicant, recruitment, assessment, career, learning and talent workflows	Consent where required, contract performance, legitimate interests, employment or programme purposes, and authorised Client or Partner instructions.
Client and Partner administration	Contract performance, legitimate interests, legal obligations, billing and account administration.
AI Services, Digital Workers and automation	Contract performance, legitimate interests, authorised instructions, consent where required, and appropriate safeguards for high-impact workflows.
Security, fraud prevention and platform integrity	Legitimate interests, legal obligations, protection of rights, and security requirements.

Platform support, training and communications	Contract performance, legitimate interests and consent where required.
Billing, payment administration, receivables and authorised financing arrangements	Contract performance, legitimate interests, legal obligations, payment administration and enforcement of rights.
Analytics, product improvement and ecosystem development	Legitimate interests, consent where required, de-identification, aggregation and platform improvement.
Compliance, audit, disputes and legal enforcement	Legal obligations, legitimate interests, protection of rights and regulatory requirements.
Marketing and business development	Consent where required, legitimate interests where permitted, and opt-out rights for direct marketing.

9. Consent and withdrawal

Where Trendi relies on consent, the relevant consent may be requested through the Platform, a workflow, a consent form, an application process, a Commercial Document, a privacy notice or another approved process. Consent is not the only lawful basis for processing. Trendi may also process Personal Information where another lawful basis applies, including contract performance, legal obligation, legitimate interest, authorised Client instruction, security, billing, compliance, dispute resolution or protection of rights.

Where applicable law gives you the right to withdraw consent, you may do so through the Platform or by contacting Trendi using the published privacy contact details. Withdrawal of consent does not affect processing that was lawful before withdrawal, or processing that continues under another lawful basis.

PART C - AI, ANALYTICS, SHARING AND TRANSFERS

Explains how Trendi uses platform intelligence, AI-enabled services and responsible sharing to operate and improve the ecosystem.

10. AI Services, Digital Workers and automated support

The Platform may use AI Services, Digital Workers, automated workflows, matching, scoring, classification, summarisation, recommendations, reporting, prompt-based tools and other decision-support features. These tools may process Personal Information where relevant to an authorised workflow.

AI outputs and automated outputs are intended to support human review, user enablement and operational efficiency. Unless expressly approved by Trendi and permitted by applicable law, they must not be used as the sole basis for high-impact employment, disciplinary, legal, medical, credit, immigration, regulatory or similarly significant decisions. Clients, Partners and Users are responsible for reviewing and validating outputs before relying on them in a decision or communication.

Trendi may monitor, test, evaluate and improve AI Services and Digital Workers using Platform Data, de-identified data, aggregated data, logs, prompts, outputs and human review records, subject to this Policy, the Platform Terms and Conditions, applicable Commercial Documents and applicable law.

Unless expressly stated in a Commercial Document, data processing notice or approved AI workflow, Trendi does not intentionally permit third-party AI providers to use identifiable Client Data for their own public model training. Where third-party AI services are used, Trendi will apply reasonable contractual, technical or organisational safeguards appropriate to the use case and the data involved.

11. Platform Data, analytics and de-identified insights

Trendi may generate and use Platform Data, analytics, logs, performance data, usage data, security data, billing data, aggregated data, anonymised data, de-identified insights and statistical information for product improvement, security, support, forecasting, reporting, benchmarking, billing, payment administration, authorised financing arrangements, compliance, ecosystem management, AI improvement, new business development and approved brand or marketing activity.

Where we use aggregated, anonymised or de-identified information, we will take reasonable steps so that it does not identify a specific person or Client, unless disclosure is otherwise permitted by this Policy, the Platform Terms and Conditions, a Commercial Document or applicable law.

12. Sharing and disclosures

Trendi does not sell Personal Information as a business model. We may share Personal Information where reasonably necessary, lawful and proportionate for the purposes described in this Policy, the Platform Terms and Conditions, a Commercial Document, a Client or Partner instruction, or applicable law. If a regional privacy law treats certain advertising or analytics disclosures as a “sale” or “share”, Trendi will provide the required notice, choice or opt-out mechanism where that law applies.

Where Trendi uses service providers, operators, processors or sub-processors, Trendi will take reasonable steps to require appropriate confidentiality, security and data protection obligations, taking into account the nature of the services and applicable law.

Recipient category	Reason for sharing
Clients, Partner Clients and Client Administrators	Authorised workspace access, reports, assessments, applicant workflows, talent workflows, Platform support and services.
Business Partners and implementation partners	Partner-Led Services, onboarding, implementation, adoption support, solution support, training, consulting, client success and other approved services, where the Partner is appointed and access is necessary.
Trendi Parties and affiliates	Operation, security, support, product improvement, administration and ecosystem governance.

Service providers / operators / processors	Cloud hosting, infrastructure, communications, analytics, payment processing, verification, assessment, security, support, ticketing, marketing operations and other contracted services.
Accredited Developers and Marketplace Participants	Only where required for approved Development Items, integrations, support, testing, marketplace functionality or maintenance, and subject to Trendi controls.
Banks, funders, cessionaries, assignees and payment participants	Billing, collections, payment administration, receivables, cessions, assignments, debtor acknowledgements, account confirmations, credit assessment, audit and authorised financing arrangements.
Professional advisers, auditors and insurers	Legal, tax, accounting, audit, insurance, compliance, governance and dispute-resolution purposes.
Regulators, courts and law enforcement	Where required or permitted by law, court order, regulatory process, investigation or to protect rights, safety and security.
Corporate transaction parties	Restructuring, merger, acquisition, investment, sale of assets, financing, due diligence or similar transactions, subject to appropriate confidentiality and privacy safeguards.

13. International transfers

The Trendi ecosystem may operate across borders. Personal Information may be hosted, accessed, supported, transferred or processed in countries other than the country where it was collected, including by Trendi Parties, cloud providers, support teams, service providers, authorised partners, payment providers, funders or other approved recipients.

Where required by applicable law, we will use appropriate safeguards for cross-border transfers. These may include contractual protections, operator or processor terms, data processing agreements, standard contractual clauses or equivalent mechanisms, transfer impact reviews, security safeguards, consent where required, or other measures appropriate to the nature of the transfer and the applicable law.

PART D - SECURITY, RETENTION, RIGHTS AND UPDATES

Explains Trendi's security approach, retention principles, user rights and policy update process.

14. Security, confidentiality and incidents

We use commercially reasonable technical and organisational measures designed to protect Personal Information against loss, unauthorised access, misuse, alteration, disclosure or destruction, taking into account the nature of the information, the processing, the risks and applicable law. These measures may include:

- access controls, role-based permissions and least-privilege access;
- password controls and multi-factor authentication where required or appropriate;
- encryption, secure hosting, backup and recovery measures where appropriate;
- logging, monitoring, vulnerability management and security review processes;
- confidentiality obligations for employees, contractors, operators, processors and service providers;
- secure development, testing, API and integration controls where applicable;
- incident response, investigation, containment and notification processes.

No platform or transmission method is completely secure. Users, Clients, Partners and Developers must also protect their own accounts, devices, credentials, integrations, workspaces and user permissions. If you suspect unauthorised access, credential compromise or a security incident, you must notify Trendi promptly through the Platform or privacy/support contact details.

Where legally required, Trendi will notify the relevant Client, Partner, End Client, data subject, regulator or other required party about a security compromise or personal data breach, taking into account applicable legal requirements, law enforcement needs and measures needed to determine the scope and restore the integrity of the system. Where Trendi acts as processor / operator and a security incident affects Client-controlled data, Trendi may notify the relevant Client or Partner so that the responsible party / controller can meet its own notification obligations.

15. Retention, deletion and anonymisation

We retain Personal Information only for as long as reasonably necessary for the purposes described in this Policy, the Platform Terms and Conditions, a Commercial Document, a Client or Partner instruction, or applicable law. Retention periods may differ by record type, role, territory, workflow, Client instruction and legal requirement.

Record type	Typical retention approach
Account, access and acceptance records	Retained while the account, workspace or legal relationship is active and for a reasonable period afterwards for audit, disputes, security, contract and compliance purposes.
Applicant, assessment, career and #MyCareer records	Retained for the period required for the relevant workflow, Client or Partner instruction, programme, legal basis or consent. Inactive records may be anonymised or deleted after a defined period, commonly 24 months unless a different period applies.
Client, Partner and Commercial Document records	Retained for the duration of the relationship and afterwards as required for billing, tax, accounting, audit, receivables, cessions, disputes and legal compliance.
Support, security and technical logs	Retained for operational, audit, security, fraud prevention, support and compliance periods appropriate to the risk and system purpose.
Aggregated, anonymised or de-identified data	May be retained for longer where it no longer identifies a person or is used for research, analytics, platform improvement or reporting.

We may anonymise, de-identify, archive, delete or restrict Personal Information when it is no longer required. We may retain records where required or permitted by law, contract, audit, tax, employment, dispute resolution, payment administration, receivables, cession, security, regulatory or legitimate business purposes.

Requests to correct, delete, anonymise or restrict assessment records, audit logs, security logs or other integrity-sensitive records may be limited where alteration would undermine accuracy, security, evidentiary value, assessment integrity, contractual obligations, regulatory obligations or the rights of another person.

16. Cookies, website technologies and direct marketing

We may use cookies, pixels, web beacons, tags, analytics tools, local storage and similar technologies to operate the website and Platform, remember preferences, secure accounts, analyse usage, improve services and provide relevant communications. Some cookies may be necessary for the Platform to function. Others may be optional or subject to consent depending on applicable law and the relevant cookie notice.

We may send administrative, service, support, security, billing and account communications where necessary for the Platform and services. We may send marketing communications where permitted by law, including where you have consented or where we are permitted to communicate with an existing customer or ecosystem participant. You may opt out of promotional communications at any time using the unsubscribe mechanism or by contacting us. Opting out of marketing does not stop service, security, account, legal or transactional communications.

Where POPIA or another applicable law requires specific consent or opt-out processes for direct marketing, Trendi will apply the relevant requirements to the applicable communication channel and data subject category.

17. Your privacy rights

Depending on the applicable law and your relationship with Trendi, you may have rights to:

- ask whether we hold Personal Information about you;
- request access to, or a copy of, your Personal Information;
- request correction or updating of inaccurate or incomplete information;
- request deletion, destruction, anonymisation or restriction where legally available;
- object to certain processing, including direct marketing;
- withdraw consent where processing is based on consent, without affecting prior lawful processing;
- request portability of certain information where applicable;
- request information about recipients or categories of recipients;
- ask for human review or challenge certain automated decisions where applicable law gives you that right;
- complain to a regulator or supervisory authority.

Some rights may be limited by law, confidentiality, legal privilege, assessment integrity, security, employment obligations, Client or Partner instructions, records retention, contractual obligations, payment administration, receivables, cessions, audit, regulatory requirements or third-party rights.

18. Requests, complaints and regulator contact

You may submit privacy requests through the Platform or by contacting Trendi using the privacy/support contact details published by Trendi. We may need to verify your identity and authority before responding. Where we process information on behalf of a Client, Business Partner or End Client, we may refer the request to that Client, Partner or End Client or coordinate with them as required by applicable law.

If you are in South Africa or POPIA applies, you may have the right to contact the Information Regulator. Current contact details should be checked on the Information Regulator’s official website. If you are in another jurisdiction, you may have the right to contact the relevant local data protection authority or supervisory authority.

19. Updates to this Policy

Trendi may update this Policy from time to time to reflect changes in the Platform, ecosystem, laws, technology, privacy practices, services, security requirements, Commercial Documents, operational structures or data processing activities. The updated Policy may be published on the Trendi website, presented through the Platform, linked in the legal centre, notified by email or incorporated into a Commercial Document.

Where required by law or Trendi policy, we may request renewed acknowledgement or acceptance. The version of this Policy that applies to a particular interaction may be evidenced by publication records, portal logs, acceptance logs, Commercial Documents or other business records.

ANNEXURES

Annexure A. Practical data map

This annexure gives examples only. The actual information processed depends on the relevant Platform workflow, Client instruction, Partner arrangement, Commercial Document, role and legal basis.

Ecosystem role	Typical information
Website visitor	IP address, device, browser, cookie identifiers, page activity, form submissions and communications.
Applicant User	Identity, contact, CV, application, qualifications, work history, skills, assessment, verification, career interest, learning and #MyCareer-related data.
Client User / Client Administrator	Identity, contact, role, workspace, permissions, usage, reports, support activity, administrator actions and acceptance logs.
Business Partner / End Client	Organisation, user, contact, commercial, implementation, billing, client-management, deal registration and payment-flow information.
Accredited Developer / Marketplace Participant	Identity, contact, credentials, accreditation, development items, API usage, technical logs, support tickets, marketplace activity and approval records.
Employee User	Identity, role, access, internal workflow, support, security, usage, training, HR or operational information depending on the organisation and workflow.
Supplier / payment participant	Identity, contact, organisation, payment, billing, tax, account, support, audit and compliance information.

Annexure B. Purposes, records and safeguards

Purpose	Typical records	Primary safeguards
Platform operation	Account, workspace, permission, access and configuration records.	Access controls, audit logs, least privilege, security monitoring.
Applicant and talent workflows	Applications, CVs, skills, assessments, qualifications, #MyCareer journeys and reports.	Lawful basis, notice, role-based access, human review, retention controls.
Client / Partner delivery	Commercial Documents, service orders, implementation records, support tickets and reports.	Contractual controls, confidentiality, workspace restrictions, Partner obligations.
AI and automation	Prompts, inputs, outputs, model or Digital Worker activity and human review records.	Human oversight, testing, access controls, data minimisation, output review.
Security and compliance	Logs, incident records, access history, device data, investigation records.	Monitoring, incident response, restricted access, regulatory notification where required.
Payment and receivables	Invoices, payment status, account confirmations, debtor acknowledgements and payment directions.	Need-to-know sharing, confidentiality, contract controls and privacy safeguards.
Product improvement and analytics	Usage, performance, aggregated, anonymised or de-identified insights.	Aggregation, anonymisation, de-identification and controlled publication.

End of Trendi Global Privacy Policy