POPIA Privacy Notice — HAHSTAG INTERNATIONAL (PTY) LTD t/a Hashtag International

Doc ID: HASHTAG-IO-01 · FINAL v1.0 · Effective 27 October 2026

Effective date: 27 October 2026 · **Version:** 1.0

This notice explains how HAHSTAG INTERNATIONAL (PTY) LTD, trading as Hashtag International ("**Hashtag**", "**we**", "**us**", "**our**") collects, uses, shares and protects personal information when you visit https://hashtagintl.com, contact us, apply for a job with us, or do business with us. It also explains our role when we process personal information on behalf of our clients.

We are based in South Africa and comply with the Protection of Personal Information Act 4 of 2013 ("**POPIA**"). Where we process information about people in the United Kingdom, Ireland, the United States, Canada, Australia or New Zealand, we also take account of the laws that apply there (such as the UK GDPR, EU GDPR, US federal/state laws, Canada PIPEDA, Australian Privacy Act 1988 and NZ Privacy Act 2020), to the extent they apply to us.

1. Who we are

Company	HAHSTAG INTERNATIONAL (PTY) LTD (trading as Hashtag International)
Registration number	2026/794619/07
Operating premises	35 Dentvale Close, Rydalvale, Phoenix, Durban, KwaZulu-Natal
Information Officer	Christopher (Chris) Naidoo — registered with the Information Regulator (Oct 2026); no Deputy IO designated
Email	chris@hashtagintl.com
Website	https://hashtagintl.com

2. Our two roles

(a) Responsible party (controller). For information about our website visitors, enquirers, prospective and current business clients, suppliers, job applicants and employees, we decide why and how it is processed. This policy mainly covers that processing.

(b) Operator (processor) for our clients. When we run outbound or customer-service campaigns, we process our clients' customer and prospect data (for example names, phone numbers, call recordings and call outcomes) **only on our clients' instructions**, usually inside the client's own dialler, CRM and telephony systems. In that case the **client** is the responsible party / controller, and the client's privacy notice governs. If you received

a call from us on behalf of a client and have a question, objection or opt-out request, tell the agent or contact us and we will pass it to the client promptly (see section 10).

3. Information we collect

Source	Information
Website contact forms, email, phone, WhatsApp	Name, company, job title, email, phone number, country, message content
Business clients and suppliers	Contact details of representatives, contract and billing information, correspondence
Job applicants	CV, contact details, ID number, qualifications, work history, references, interview notes, assessment results, and — with your consent or where the law allows — criminal and credit checks
Website technical data	IP address, browser and device type, pages viewed, referring site, dates and times, cookie identifiers

We do not knowingly collect personal information from children (under 18) through our website.

4. Why we use it, and our lawful basis

Purpose	Lawful basis (POPIA s11)
Responding to enquiries and preparing proposals	Necessary to take steps at your request before a contract; legitimate interest
Providing and billing for our services; managing supplier relationships	Performance of a contract
Recruitment and employment	Steps before / performance of a contract; legal obligation; consent where required (e.g. background checks)
Complying with tax, labour, exchange-control and other laws	Legal obligation
Website security, analytics and improvement	Legitimate interest; consent for non-essential cookies where required
Sending business-to-business information about our services	Legitimate interest or consent, as the law requires; you can opt out at any time

5. Direct marketing

We market our services to businesses. We will not send you unsolicited electronic marketing (email, SMS, automated calls) in breach of section 69 of POPIA, the UK Privacy and Electronic Communications Regulations, Irish ePrivacy rules or US rules. Every marketing message will tell you how to opt out, and we will honour opt-outs promptly. To opt out, email chris@hashtagintl.com with "Unsubscribe" in the subject line.

6. Cookies

Our website may use essential cookies (needed for the site to work) and, if enabled, analytics cookies to understand how the site is used. We will list any analytics tool we enable on this page.. Where required by law (e.g. for UK and Irish visitors), we will ask for your consent before setting non-essential cookies. You can also block or delete cookies in your browser settings.

7. Who we share information with

We do not sell personal information. We share it only with:

- service providers who support our business (website hosting, email and cloud software, IT support, payroll, accounting, banking, recruitment and screening, legal and professional advisers), under confidentiality and data-protection obligations;
- our clients, where relevant to the services (for example, the names of agents assigned to a client's campaign);
- authorities where required by law (e.g. SARS, Department of Employment and Labour, law enforcement with a valid legal request);
- a buyer or investor in the event of a sale, merger or restructuring, under confidentiality.

8. International transfers

We serve clients in the UK, Ireland, USA, Canada, Australia and New Zealand, and some of our service providers store data outside South Africa. When we transfer personal information outside South Africa we do so in line with section 72 of POPIA — for example where the recipient is bound by law or a binding agreement giving adequate protection, where you consent, or where the transfer is necessary to perform a contract with you or in your interest. For UK and EU personal information processed for our clients, we support the transfer safeguards our clients need (such as the UK International Data Transfer Agreement or Addendum, or EU Standard Contractual Clauses).

9. How long we keep information

We keep personal information only as long as needed for the purpose for which it was collected, or as required by law. As a guide:

- Enquiries that do not lead to business: up to 24 months.
- Client and supplier contracts and financial records: at least 5 years after the end of the relationship (tax and company law).
- Unsuccessful job applications: up to 12 months, unless you agree to longer.
- Employee records: for the period required by labour and tax law (generally at least 3–5 years after employment ends).
- Client campaign data processed as operator: as instructed by the client, and returned or deleted at the end of the engagement.

10. Your rights

Subject to the law, you may:

- ask whether we hold personal information about you and request access to it (see our PAIA Manual);
- ask us to correct, update or delete inaccurate, irrelevant, excessive, out-of-date, incomplete, misleading or unlawfully obtained information;
- object to processing based on legitimate interest, and object at any time to direct marketing;

- withdraw consent (without affecting earlier lawful processing);
- complain to the Information Regulator.

If you are in the UK, Ireland or a US state with its own privacy law, you may have additional rights under that law; contact us and we will help.

To exercise any right, email chris@hashtagintl.com. We may need to verify your identity. Where we hold your information only as an operator for a client, we will forward your request to that client and assist them in responding.

Information Regulator (South Africa): Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, 2191 · 010 023 5200 · POPIAComplaints@inforegulator.org.za · https://inforegulator.org.za

UK residents may also contact the Information Commissioner's Office (https://ico.org.uk); Irish residents the Data Protection Commission (https://www.dataprotection.ie).

11. Security

We use reasonable technical and organisational measures to protect personal information against loss, damage, unauthorised access or destruction — including access controls, unique log-ins, multi-factor authentication where available, restricted use of personal devices on the production floor, staff confidentiality undertakings and training, and supplier due diligence. No system is completely secure; if we have reasonable grounds to believe your personal information has been accessed or acquired by an unauthorised person, we will notify the Information Regulator and you as required by section 22 of POPIA (and, where we act as operator, we will notify the client immediately).

12. Changes to this policy

We may update this policy from time to time. The current version will always be on our website with its effective date.

Annex — POPIA operator posture (summary for clients)

This annex summarises how Hashtag behaves when processing client data. The binding terms are in our Master Services Agreement and Data Processing Agreement.

1. **Instructions only.** We process client personal information only with the client's knowledge or authorisation and for the client's documented purposes (POPIA s20).
2. **Written contract.** Every client engagement is covered by a written agreement requiring us to maintain security safeguards (POPIA s21 read with s19).
3. **Client systems by default.** Clients provide the dialler, data and VoIP. Data stays in client systems wherever possible; agents do not export, download or copy lists.
4. **Confidentiality.** All staff sign confidentiality and POPIA undertakings and receive training before accessing client systems.
5. **Breach notification.** We notify the client immediately, and in any event within 24 hours of becoming aware of a suspected security compromise (POPIA s21(2)), and help the client meet its own notification duties.
6. **Data-subject requests and opt-outs.** Requests and do-not-call/opt-out instructions received by agents are logged and passed to the client within 1 business day; agents follow client suppression processes during calls.
7. **Sub-operators.** We do not engage another operator to process client data without the client's prior written consent.
8. **Return or deletion.** At the end of an engagement we return or delete client data and remove our access to client systems, as the client instructs.
9. **Compliance responsibility for data and campaigns.** The client is responsible for the lawfulness of the data supplied (including consent and screening against the

TPS/CTPS, Irish National Directory Database preferences, the US National Do Not Call Registry and state lists, and South African opt-out registers where applicable) and for compliant scripts, calling hours and disclosures. Hashtag is responsible for following the client's documented instructions and scripts.