Privacy Policy

How Axiom Process Technology handles the information entrusted to us. POPIA-aligned data protection practices for our industrial intelligence engagements.

We work with industrial data, which means we operate at the boundary of operational technology and information technology. The information our clients share with us, whether commercial, technical, or personal, sits inside a posture of restraint, governance, and traceability. This page tells you exactly what we collect, why we collect it, what we do with it, and the rights you hold in relation to it.

01. Scope and who we are

This policy explains how **Axiom Process Intelligence (Pty) Ltd**, trading as Axiom Process Technology, collects, uses, stores, shares, and protects personal information. It applies to information we obtain through our website, our commercial communications, our active client engagements, and any other interaction you have with us in our capacity as a process intelligence consultancy operating from the Republic of South Africa.

Axiom Process Intelligence (Pty) Ltd is a private company registered with the Companies and Intellectual Property Commission (CIPC). For the purposes of the Protection of Personal Information Act, 2013 (POPIA), Axiom is the responsible party in respect of personal information we determine the purpose and means of processing. Where we process personal information on behalf of a client under a written engagement, we act as an operator and are bound by the client's instructions and the protections required under section 21 of POPIA.

This policy does not apply to third-party websites, services, or applications that may be linked to from our site or referenced in our work product. Each such third party operates under its own privacy posture.

02. Information we collect

The personal information we collect is narrow, purposeful, and tied to specific lawful bases. We do not collect information speculatively. The categories below describe what we may collect across different interaction surfaces.

- **Identification and contact information** Name, role, employer, business telephone number, business email address, postal address, and country, provided when you contact us, complete a scoping enquiry, or accept an engagement document.
- **Engagement and commercial information** Information shared in the course of pre-contract discussions and active engagements, including non-disclosure agreement counterparts, statements of work, change requests, and meeting records.
- **Communications** Email correspondence, signed letters, voice notes left for us, and message threads on professional platforms where you have initiated contact with us.
- **Technical information about your visit** IP address, browser type and version, operating system, referring page, the pages you view on our site, and the date and time of access. This information is logged at the web-server level and is used for security, performance, and aggregate analytics.
- **Recruitment information** Where you apply for a position with us, the curriculum vitae you supply, work history, qualifications, references you have nominated, and any portfolio material you choose to share.

We do not knowingly collect special personal information as defined under section 1 of POPIA (such as health information, biometric information, or political affiliation) unless you choose to share it in a recruitment context and it is necessary for the purpose. We do not collect personal information of children, and our services are not directed at children.

03. How we collect it

We collect personal information directly from you in nearly every case. The collection mechanisms are:

- **Contact forms on this website** when you submit a scoping enquiry or general message.
- **Direct correspondence** by email to our published business addresses, by telephone to our published numbers, or in person at meetings you have arranged with us.
- **Engagement documentation** exchanged during commercial scoping, contract negotiation, and active project execution.
- **Professional networking platforms** such as LinkedIn, where you have initiated outreach to a named member of the Axiom team.
- **Server logs** generated automatically by your interaction with our website.

Where we receive personal information from a third party (for example, a referee you have nominated during a recruitment process), we collect only what is necessary for the stated purpose and we treat that information under the same protections as information collected directly from you.

04. Why we process it

Every category of processing we undertake has at least one lawful basis under section 11 of POPIA. The principal purposes are listed below alongside their basis.

- **To respond to enquiries you have initiated** Lawful basis: your consent, given by initiating the contact, and our legitimate business interest in responding professionally to commercial enquiries.
- **To negotiate, agree, and perform our engagements** Lawful basis: the conclusion or performance of a contract to which you, or the entity you represent, is a party.
- **To meet professional, regulatory, and statutory obligations** Lawful basis: compliance with an obligation imposed by law, including company law, tax law, and any sector-specific requirements applicable to our engagements.
- **To assess and respond to job applications** Lawful basis: steps taken at your request prior to entering into a contract of employment.
- **To operate and secure our website and internal systems** Lawful basis: our legitimate interest in providing a stable, secure web presence and protecting our infrastructure from misuse.
- **To improve our service and how we communicate** Lawful basis: our legitimate interest in understanding how our site is used and which of our offerings resonate, balanced against any limited impact on you.

We do not engage in profiling, automated decision-making, or targeted advertising on the basis of personal information collected through our website. We do not sell personal information to any third party, under any circumstance.

05. Who we share it with

We share personal information sparingly and only with parties bound to protect it. The categories of recipients are:

- **Internal Axiom personnel** Members of the Axiom team who require access to the information to perform the engagement or function for which it was collected, subject to internal access controls.
- **Authorised operators** Trusted technology providers we engage to host our infrastructure, transmit our communications, or support our internal operations. Each operator is bound by a written agreement that obliges them to process personal information only in accordance with our instructions and to maintain appropriate technical and organisational safeguards.
- **Professional advisors** Our legal counsel, auditors, accountants, and insurance brokers, where disclosure is necessary for the proper conduct of those professional services.
- **Regulators, courts, and statutory authorities** Where disclosure is required by law, court order, or the exercise of a regulatory power, we will comply, while challenging requests that we consider over-broad or unlawful.
- **Successors in a business transition** In the event of a sale, merger, restructuring, or financing event, personal information may be transferred to a successor entity, subject to the protections of POPIA and the terms of this policy.

06. Cross-border transfers

Some of the operators that support our infrastructure (for example, our email and cloud services) are located outside the Republic of South Africa. Where personal information is transferred to a third country, the transfer is undertaken in accordance with section 72 of POPIA. We rely on one or more of the following grounds:

- The recipient is subject to a law, binding corporate rules, or binding agreement that provides an adequate level of protection comparable to that required under POPIA.
- The transfer is necessary for the performance of a contract between you and Axiom, or for the implementation of pre-contractual measures taken at your request.
- The transfer is necessary for the conclusion or performance of a contract concluded in your interest between Axiom and a third party.

You may request, in writing, a summary of the safeguards in place for any particular cross-border transfer that affects your personal information.

07. How long we keep it

We retain personal information only for as long as it is necessary for the purpose for which it was collected, or for as long as the law requires us to keep it, whichever is longer. The principal retention periods are:

- **Enquiry correspondence that does not progress to engagement:** retained for up to 24 months, after which it is deleted or anonymised.
- **Engagement records (contracts, scopes of work, deliverables, correspondence):** retained for at least 5 years from the conclusion of the engagement, in line with the prescription period

under the Prescription Act, and longer where tax or company-law obligations require.

- **Tax and financial records:** retained for at least 5 years from the end of the tax period to which they relate, as required by the Tax Administration Act.
- **Recruitment records for unsuccessful applications:** retained for 12 months from the conclusion of the recruitment process, after which they are deleted, unless you have consented to a longer retention period for future opportunities.
- **Server logs:** retained for 90 days, after which they are aggregated for security analytics or deleted.

Where the law permits and there is no overriding legal obligation to retain, we will delete or anonymise personal information at your request.

08. How we protect it

We implement the technical and organisational safeguards required under section 19 of POPIA. These include encryption of data in transit and at rest, role-based access controls on every system that holds personal information, multi-factor authentication for all administrative access, segregated environments for production and development workloads, regular software patching, monitored backups, and a documented incident response procedure.

Where we engage operators to process personal information on our behalf, we require them to maintain a substantively equivalent security posture and we audit that posture at engagement onboarding and on a periodic basis thereafter.

09. Your rights under POPIA

You hold a defined set of rights in respect of the personal information we process about you. You may exercise any of these rights by contacting our Information Officer using the details in section 13 below. We will respond within a reasonable period and free of charge, unless the law specifies otherwise.

- **The right to be notified** That we are processing your personal information and the purposes for which we are processing it. This policy is itself a primary notification.
- **The right of access** To request confirmation of whether we hold personal information about you, and to receive a record of that information.
- **The right to correction or deletion** To request correction of inaccurate, irrelevant, excessive, out-of-date, incomplete, misleading, or unlawfully obtained personal information.
- **The right to object** To object, on reasonable grounds, to the processing of your personal information, including processing on the basis of legitimate interest.
- **The right to withdraw consent** Where processing is based on consent, to withdraw that consent at any time, without affecting the lawfulness of processing carried out prior to withdrawal.
- **The right to complain** To submit a complaint to the Information Regulator if you believe your rights have been infringed.

The Information Regulator can be reached at the JD House, 27 Stiemens Street, Braamfontein, Johannesburg 2001, by post at PO Box 31533, Braamfontein 2017, by email at , or via the regulator's website at inforegulator.org.za. We encourage you to raise concerns with us first so we have an opportunity to address them directly.

10. Cookies and similar technologies

Our website uses cookies sparingly. We deploy only those cookies that are strictly necessary to operate the site, plus a limited set of analytics cookies that help us understand which pages are useful and where visitors run into friction. We do not use advertising cookies, retargeting pixels, or third-party tracking beacons.

- **Strictly necessary cookies:** set by our infrastructure to deliver the site, remember your interaction preferences during a session, and protect the site from misuse. These cannot be disabled without affecting functionality.
- **Analytics cookies:** set, if at all, to aggregate, non-identifying visit metrics. We use these to understand traffic patterns and improve the site.

You can configure your browser to block or delete cookies. Doing so may affect parts of the site that rely on session continuity. The settings to do this are typically found under the Privacy or Security section of your browser preferences.

11. Information from client engagements

Our engagements frequently involve access to client operational data, including SCADA tags, historian extracts, laboratory results, maintenance records, and process documentation. This data is the property of the client and is governed primarily by the engagement contract and any related non-disclosure agreement, not by this privacy policy.

Where such data incidentally contains personal information (for example, the names of plant operators or shift supervisors associated with historian timestamps), we treat that information under the same protections set out in this policy. We do not republish, repurpose, or share client operational data outside the scope of the engagement that produced it, and we apply contractually-defined retention and destruction obligations at engagement close.

Any case study, conference paper, or marketing reference that derives from a client engagement is anonymised by default and is published only with explicit, written client consent.

12. Changes to this policy

We may update this policy from time to time to reflect changes in our practice, the services we offer, the law, or the expectations of the regulators we answer to. Material changes will be communicated through a clearly-marked notice on this page and, where appropriate, directly to active clients and engagement counterparts. The effective date at the top of this page indicates when the current version came into force. We encourage you to revisit this page periodically.

13. How to contact us

For any question, request, or concern relating to this policy or to the personal information we hold about you, please contact our Information Officer using the details below. We aim to acknowledge enquiries within 5 business days and to substantively respond within the timelines required by POPIA.