

DisputeSolve Privacy Policy

Last updated: 22 October 2026

1. Introduction

This Privacy Policy explains how DisputeSolve processes personal information when people visit www.disputesolve.com, register an account, complete an initial questionnaire, liaise with DisputeSolve personnel or consultants, submit dispute information, or request referral to an alternative dispute resolution consultant. It applies to personal information about identifiable living individuals and, where applicable, identifiable existing juristic persons under the Protection of Personal Information Act 4 of 2013 ("POPIA").

"DisputeSolve", "we", "us" and "our" mean the legal entity operating the website and services, identified in section 3. This policy is supplemented by any specific notice given when information is collected or a service is arranged.

Registering, using the platform or acknowledging this policy does not itself constitute consent to every processing activity. Where consent is required, we obtain a voluntary, specific and informed expression of will separately. This policy does not waive statutory rights.

2. What personal information may be processed

At registration, we process the account, identification and contact information requested by the registration form, together with information needed to authenticate users and administer accounts. Depending on the services requested, we may subsequently process correspondence, billing and transaction records, dispute facts, supporting documents and relevant information about representatives, counterparties, witnesses and other persons.

The initial questionnaire is designed to obtain general information about the matter and assistance sought without requesting names or identifying details about other parties, sensitive information or supporting documents. Users should not include those details at this stage. Responses linked to a registered account may nevertheless constitute personal information and are protected accordingly. The questionnaire is not described as anonymous merely because it does not ask for names.

During later liaison or a further dispute submission, information may include special personal information or children's information. We process it only where the additional requirements in section 15 are met. Users

should provide only material reasonably necessary for the requested service and lawfully permitted to be supplied, omitting or redacting unrelated third-party details where practicable.

Website and platform operations may also generate device, browser, IP address, login, file-metadata and technical-log information. Any cookies or similar technologies actually used are addressed in section 6. We limit processing to information adequate, relevant and not excessive for the applicable purpose.

3. Responsible party and Information Officer

The responsible party is the person or organisation that, alone or together with others, determines the purpose of and means for processing personal information. For the account-management, intake, assessment and referral processing that DisputeSolve determines, the responsible party is Disputesolve (Pty) Ltd, registration number 2022/275369/07, trading as DisputeSolve,. The Information Officer is Ferdie Lochner, email popi@disputesolve.com, telephone +27844443643.

DisputeSolve does not become merely an operator because a client supplies information. Personnel processing under our direct authority do so within our responsibilities. An external provider processing solely on our behalf under a contract or mandate may be an operator. An independently engaged arbitrator, mediator, negotiator or other professional may be a separate responsible party for processing that the professional determines. These roles depend on actual functions, not contractual labels alone.

Where a particular service involves processing solely on another responsible party's behalf, or purposes and means determined in conjunction with another party, we will explain the relevant arrangement in the service terms or an additional notice. None of these arrangements removes a party's applicable statutory responsibilities.

4. Sources of personal information

We collect information directly through registration, questionnaires, communications, consultations and further dispute submissions. We may also receive relevant information from clients about other persons, and from representatives, alternative dispute resolution consultants, service providers, public records or other lawful sources.

Indirect collection must be justified by an applicable exception in section 12 of POPIA. We take reasonably practicable steps to give the notice required by section 18 before direct collection or as soon as reasonably practicable after indirect collection. A specific notice may supplement this policy.

Any exception to notification is assessed for the particular processing. There is no blanket exemption simply because information concerns a dispute. Exceptions concerning proceedings before a court or tribunal are not automatically applied to every preliminary consultation or informal negotiation.

The platform may generate operational records, including account activity, support records and technical logs, for lawful administration, security, fraud prevention or evidentiary purposes, subject to appropriate retention limits.

5. Lawful bases and purposes of processing

We identify an applicable section 11 justification for each processing purpose. Depending on the circumstances, this may be consent; necessity for concluding or performing a contract to which the data subject is a party; compliance with a legal obligation; protection of the data subject's legitimate interests; or necessity for pursuing our legitimate interests or those of a third party to whom information is supplied.

A client's contract or authorisation does not automatically justify processing about another person, and a client cannot consent on behalf of an opposing party or witness merely by submitting their details. Where legitimate interests are relied on, we consider necessity, proportionality, the impact on affected persons and less intrusive alternatives. Special personal information and children's information require the further authorisations described in section 15 of POPIA.

Personal information may be processed for the following purposes, where supported by the applicable justification:

- creating, authenticating and administering accounts and providing service communications;
- using the initial questionnaire to understand the general nature of a matter and the assistance sought;
- liaising with clients, assessing further dispute information and supporting intake and administration;
- identifying suitable arbitrators, mediators, negotiators or other alternative dispute resolution consultants, checking expertise, availability and conflicts, and arranging lawful referrals or engagements;
- processing payments and maintaining financial and other legally required records;
- maintaining security, administering systems, detecting misuse and investigating suspected unlawful activity;

- establishing, exercising or defending legal rights or obligations, handling requests and complaints, and responding to lawful regulatory or judicial requirements;
- improving services using properly de-identified information where practicable, or identifiable information only where separately lawful and necessary; and
- conducting direct marketing only where permitted as described in section 7.

Collection notices or the relevant forms will explain which information is mandatory or voluntary, any applicable legal requirement and the consequences of not providing it. Information essential to an account or requested service may be needed before that service can be provided. Optional marketing consent is not a condition of an unrelated service. Further processing must be compatible with the original purpose or otherwise permitted by POPIA.

If automated decision-making is introduced, we will assess section 71 of POPIA before making decisions based solely on automated processing that have legal consequences or affect a person to a substantial degree. Any such processing must be legally permitted, explained through an appropriate notice and accompanied by the required safeguards. An initial questionnaire does not by itself mean that a legally significant automated decision is made.

6. Cookies, analytics and online tracking

The website may use cookies or similar technologies, including browser storage, for functions such as authentication, security and remembering preferences. Their actual use, providers, purposes and duration must be accurately described in the website's cookie information. Account registration alone does not establish which technologies are used.

Where these technologies process personal information, an applicable POPIA justification is required. Optional analytics, advertising or tracking will not be treated as automatically authorised by this policy or by continued browsing. Where consent is required, the relevant technology will not be activated before an affirmative choice, and consent may be refused or withdrawn.

Any cookie notice or preference controls must reflect the technologies actually deployed. This policy does not represent that a particular cookie-management tool, analytics service or advertising pixel is installed. Browser settings may provide additional controls, although disabling technologies necessary for authentication or security may affect functionality.

7. Direct marketing

Account and service communications are distinct from promotional communications. Where we conduct direct marketing, we comply with POPIA and applicable Consumer Protection Act requirements. Our unsolicited electronic-marketing controls cover email, SMS, messaging services and telephone marketing in accordance with applicable law and the Information Regulator's guidance.

Electronic direct marketing requires consent unless the limited existing-customer exception in section 69(3) of POPIA applies. That exception requires contact details obtained in the context of a sale, marketing of our own similar products or services, and a reasonable opportunity to object free of charge and without unnecessary formality both at collection and with each communication. Registration alone does not establish every condition of this exception.

Where section 69(2) of POPIA permits it, we may approach a person only once to request consent if consent has not previously been withheld. Consent requests will comply with amended regulation 6 through a substantially similar Form 4 or another permitted, accessible method. Telephonic and automated-call consent requests will be recorded as required, with a recording or transcription made available free on request.

Marketing communications will identify the sender or principal and give a simple way to stop further messages. We retain limited suppression records to honour objections, refusals and withdrawals. Applicable pre-emptive opt-out arrangements and other consumer-protection restrictions do not replace POPIA's consent requirements. Non-electronic marketing requires a lawful justification and remains subject to the right to object.

8. Disclosure of personal information

Authorised DisputeSolve personnel and contracted providers may access information only as needed for their functions. Relevant disclosures may also be made to professional advisers, payment and hosting providers, selected alternative dispute resolution consultants, regulators, courts or other legally entitled recipients where necessary and lawful.

Referral is not permission to circulate an entire dispute file to every consultant in our database. Wherever practicable, initial suitability enquiries will use a non-identifying summary. If identities are needed to check conflicts, disclosure will be limited to the information reasonably necessary for that check. More detailed material will be shared with selected consultants only where necessary and lawful for the proposed or agreed engagement.

We will explain the proposed referral to the client and obtain instructions or authorisation where appropriate. Client approval does not replace the need for a lawful basis for processing other people's information. We consider relevance, confidentiality, privilege and procedural restrictions, and use redaction, limited extracts and restricted access where appropriate. We do not publish identifiable dispute material merely because it has been submitted.

Before sharing personal information with an independent alternative dispute resolution consultant, we will have an appropriate agreement addressing permitted purposes, confidentiality, security, restrictions on onward disclosure, incident coordination, retention and applicable rights requests. Where the consultant is a separate responsible party, the consultant remains responsible for the processing that it determines. The agreement does not guarantee that a breach can never occur, make an otherwise unlawful disclosure lawful, or relieve either party of statutory obligations.

Providers acting as our operators must process only with our knowledge or authorisation, preserve confidentiality and establish and maintain the section 19 safeguards through the written contract required by section 21 of POPIA. They must notify us immediately where there are reasonable grounds to believe that information has been accessed or acquired by an unauthorised person. Downstream processing must be appropriately authorised and protected.

We do not sell personal information or disclose it to unrelated parties for their independent marketing without an applicable lawful basis and any consent required by law.

9. Cross-border transfers

Hosting, software, backup or professional services may involve processing outside South Africa. Before transferring personal information to a third party abroad, we establish an applicable section 72 basis. Where relying on adequate protection, the recipient must be subject to a law, binding corporate rules or a binding agreement effectively upholding substantially similar reasonable-processing principles and substantially similar restrictions on onward transfers.

Consent, contractual necessity and other section 72 grounds apply only where their specific statutory conditions are satisfied. We assess the recipient, destination, safeguards and onward transfers; a foreign provider's convenience or privacy policy alone is insufficient. Relevant details will be provided through collection notices or on request.

Where section 57 of POPIA requires prior authorisation, including qualifying transfers of special personal information or children's information to a third party in a country without adequate protection, we comply with sections 57 and 58 before commencing that processing unless a lawful exception applies. We also

assess other potentially relevant prior-authorisation categories, including qualifying processing of criminal-behaviour information on behalf of third parties.

10. Security safeguards

We establish and maintain appropriate, reasonable technical and organisational measures to protect personal information against loss, damage, unauthorised destruction and unlawful access or processing. We identify reasonably foreseeable internal and external risks, maintain safeguards, regularly verify effective implementation and continually update measures in response to new risks or deficiencies, having due regard to generally accepted information-security practices.

Safeguards appropriate to the risks may include restricted account and matter access, multi-factor authentication, encryption, secure hosting, logging, patching, protected backups and restoration testing, staff confidentiality and awareness, physical protection, vendor assessment and incident-response procedures. Sensitive submissions and consultant disclosures receive protection appropriate to their content and purpose.

The Information Officer coordinates the applicable compliance framework and impact assessments with those implementing safeguards. No system is entirely immune to compromise; this does not diminish our statutory duties or waive remedies. Users should protect credentials and report suspected misuse promptly to the contact in section 18.

11. Security compromise notifications

Where there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, we notify the Information Regulator and affected data subjects as required by section 22. Regulator reporting follows its prescribed eServices process. Affected-person notification follows the statutory requirements, including the provisions concerning unknown identities and lawful delay.

Notification is made as soon as reasonably possible after discovery, taking account of legitimate law-enforcement needs and measures reasonably necessary to establish the scope and restore system integrity. We do not apply a materiality or high-risk threshold not provided by POPIA. Delay of data-subject notification on grounds contemplated in section 22(3) requires the relevant statutory determination.

Notices provide sufficient information for protective steps, including possible consequences, measures taken or intended, recommended action and the unauthorised person's identity if known. Available information is supplemented as appropriate. We coordinate with independent consultants without

assuming their separate duties, and, where acting as an operator, notify the relevant responsible party immediately under section 21(2).

12. Retention and deletion

We retain information only for as long as necessary for its purpose or another basis permitted by section 14, including a legal retention requirement, lawful operational need, contractual retention requirement or valid consent. Account records, questionnaire responses, consultation correspondence, dispute submissions and referral records may require different retention periods. A dispute does not justify indefinite retention of every document.

Records used to make decisions about a person are retained for the period prescribed by law or an applicable code, or otherwise for a period allowing a reasonable opportunity to request access. Processing is restricted where section 14 requires, including relevant cases involving disputed accuracy or evidentiary preservation.

When retention is no longer authorised, we destroy, delete or de-identify information as soon as reasonably practicable. Identifiable backups remain protected and are removed through controlled retention cycles, subject to lawful preservation. Account closure does not automatically require deletion of records that must lawfully be retained. Independent consultants may have separate lawful retention duties explained in their applicable notices.

13. Data subject rights

Subject to applicable legal limitations, data subjects have the right to:

- obtain, free of charge after adequate proof of identity, confirmation of whether we hold their personal information;
- request access to their information and relevant information about third-party recipients, subject to applicable procedures, fees and refusal grounds;
- request correction or deletion of inaccurate, irrelevant, excessive, out-of-date, incomplete, misleading or unlawfully obtained information, and destruction or deletion of records no longer authorised for retention;
- object on reasonable grounds relating to their particular situation to processing under section 11(1)(d) to (f), unless legislation provides for it, and object to direct marketing as provided by law;

- withdraw consent without affecting lawful earlier processing or another applicable justification;
- exercise applicable protections concerning solely automated decisions under section 71; and
- complain to the Information Regulator and exercise remedies available under POPIA.

Objections and correction, deletion or destruction requests are free and may be submitted through reasonably accessible channels, including the email in section 18. Other channels will be made available or assisted where required by the amended Regulations; we do not require a messaging channel that is not actually operated. A substantially similar Form 1 or Form 2 may be used rather than the original form. Telephonic requests will be recorded where required, with a recording or transcription available free on request.

We respond within applicable statutory periods, provide the required written outcome and assist where reasonably needed. As a service commitment, we aim to provide a substantive response to correction or deletion requests within 30 days. Access requests follow applicable POPIA and PAIA procedures and lawful extensions. Verification will be proportionate.

Access may be lawfully limited to protect third-party privacy, privilege or another recognised interest, with reasons and remedies explained where required. A client's account access is not an unrestricted entitlement to another person's information or a consultant's entire professional file. We will assist in directing requests concerning independently determined consultant processing to the appropriate responsible party.

14. Accuracy and user responsibilities

We take reasonably practicable steps, having regard to purpose, to keep information complete, accurate, not misleading and updated where necessary. We distinguish allegations and opinions from established facts. Users should notify us of inaccuracies and changes to their details.

Users must provide information lawfully, avoid irrelevant or excessive submissions, respect confidentiality and applicable notice requirements, and obtain consent where legally required. They should not submit sensitive evidence through the neutral questionnaire. We may seek clarification, restrict access or request redacted material. These responsibilities do not transfer or exclude our own POPIA duties.

15. Children's information and special personal information

Special personal information is subject to the prohibition in section 26 of POPIA and an applicable authorisation under sections 27 to 33 of POPIA, or from the Regulator. It includes protected information concerning health or sex life, religious or philosophical beliefs, race or ethnic origin, trade union

membership, political persuasion, biometrics and criminal behaviour. An ordinary legitimate-interest justification alone does not remove the prohibition.

Where relevant, section 27(1)(b) may authorise processing necessary to establish, exercise or defend a right or obligation in law. We assess the particular purpose and necessity: a dispute does not provide blanket permission for sensitive collection or circulation. Relevant redaction, confidentiality and access restrictions remain necessary.

Children's information requires a separate section 35 authorisation, such as prior consent of a competent person or necessity to establish, exercise or defend a right or obligation in law. Where information falls into both categories, both sets of requirements must be met.

Where our role and activities fall within the Regulations relating to the Processing of Data Subjects' Health Information by Certain Responsible Parties, 2026, we apply their additional requirements. Their applicability is assessed for the processing and role concerned, not presumed merely because a dispute document mentions health. We assess any required prior authorisation before processing starts.

16. Third-party websites and services

Links or referrals may lead to independent websites, payment services or professional services. Their own notices apply to the processing they determine. We will explain relevant consultant roles when arranging a referral or engagement.

This does not exclude our responsibility for our disclosures, operators we appoint or safeguards required by law. A provider's status depends on its actual functions. Submission to our platform does not automatically authorise every third-party use.

17. PAIA manual and access to records

We must maintain and make available the manual required of us under section 51 of the Promotion of Access to Information Act 2 of 2000 ("PAIA"). The manual must contain current contact details and prescribed access and processing information and be available through the required channels, including our website where applicable and the Information Officer.

This policy does not replace the PAIA manual. Access requests are assessed under applicable POPIA and PAIA provisions, including refusal grounds, third-party procedures and rules for records sought for legal proceedings. Amendments removing manual-related provisions from the POPIA Regulations did not abolish the separate PAIA obligation.

18. Complaints and contact details

Contact the Information Officer at popi@disputesolve.com or through the telephone details in section 3 for privacy questions, requests, objections or complaints. We will assist with reasonably accessible alternatives and explain the information needed to act.

A complaint may also be lodged directly with the Information Regulator; contacting us first is not a condition of that right. Current complaint channels, forms and assistance are available at <https://inforegulator.org.za> and <https://eservices.inforegulator.org.za>. General enquiries may be addressed to enquiries@inforegulator.org.za. Persons entitled to complain include data subjects and qualifying representatives or other persons acting as permitted by POPIA and its Regulations.

19. Changes to this policy

We may update this policy to reflect changes in law, applicable guidance, technology, services or processing. The current version and effective date will be published on the website. Where required, further notice will be given before materially different processing starts, and fresh consent obtained where existing consent does not cover it.

Continued use is not treated as consent to new processing requiring consent. Policy changes do not retrospectively remove statutory rights or make earlier unlawful processing lawful.