

DisputeSolve Privacy Policy

Last updated: 25 June 2026

1. Introduction

This Privacy Policy explains how DisputeSolve processes personal information when users visit the website, use the platform, communicate with DisputeSolve, submit enquiries, create accounts, upload dispute-related information, request services, or otherwise interact with the business. The policy is intended to support compliance with the Protection of Personal Information Act 4 of 2013 ("POPIA") and related South African legal requirements.

For purposes of this policy, "DisputeSolve", "the platform", "the website", "we", "us" and "our" refer to the DisputeSolve website and platform and the legal entity operating it. The current website address is www.disputesolve.com.

By using the website or platform, a user acknowledges this policy. Where consent is required by law for particular processing activities, DisputeSolve will seek that consent separately and in an appropriate form.

2. What personal information may be processed

Depending on the nature of the interaction, DisputeSolve may process identification and contact details, account and profile information, correspondence, billing details, records of transactions, dispute-related facts and documents, device and browser information, log information, IP address information, approximate location data, cookie-related data, and any other information reasonably necessary to provide the platform and its services.

Where the platform is used for dispute resolution or referral to subject-matter experts, the information processed may include information supplied by users about counterparties, representatives, witnesses, service providers, employees, and other persons relevant to the dispute. Users should only upload or submit personal information that is reasonably necessary for the dispute or service requested and that they are lawfully permitted to provide.

DisputeSolve may also process special personal information or children's information where this is necessary for a lawful purpose and permitted by POPIA, for example where a dispute necessarily involves health information, biometric evidence, criminal conduct allegations, or information about minors. In such cases, DisputeSolve will apply additional safeguards and rely only on a lawful basis recognised under POPIA.

4. Sources of personal information

DisputeSolve may collect personal information directly from users, from communications sent to DisputeSolve, from forms completed on the website or platform, from uploaded documents, from cookies and similar technologies, from service providers acting on behalf of users, and from third parties where this is reasonably necessary for the service or dispute-handling process.

Information may also be generated through use of the platform itself, including login history, transaction records, support tickets, audit trails, file metadata, and technical logs. This operational information may be necessary for security, system administration, fraud prevention and evidentiary recordkeeping.

5. Lawful bases and purposes of processing

DisputeSolve will process personal information only where there is a lawful basis to do so under POPIA. Depending on the context, the relevant basis may include consent, the conclusion or performance of a contract, compliance with an obligation imposed by law, protection of a legitimate interest of the data subject, the proper performance of a public law duty by a public body, or the legitimate interests of DisputeSolve or a third party, where recognised in law.

Personal information may be processed for one or more of the following purposes:

- providing access to the website, platform and user accounts;
- verifying identity and user credentials;
- facilitating dispute intake, triage, referral, administration and resolution support;
- communicating with users, experts, service providers and counterparties;
- processing payments and maintaining financial records;
- maintaining platform security, monitoring performance and detecting misuse or unlawful activity;
- complying with legal, regulatory, audit, risk-management and recordkeeping obligations;
- responding to requests, complaints, data-subject requests and lawful demands from regulators or courts;
- conducting internal reporting, service improvement, testing and analytics on a de-identified or aggregated basis where appropriate;
- sending service notices and, where legally permitted, marketing or updates about services.

DisputeSolve will take reasonably practicable steps to ensure that the personal information processed is adequate, relevant and not excessive for the stated purpose, consistent with POPIA's processing limitation and purpose specification principles.

6. Cookies, analytics and online tracking

The website may use cookies, pixels, analytics tools and similar technologies to remember preferences, keep users logged in, understand website usage, improve performance, and support security. Some cookies are strictly necessary for the functioning of the site, while others may be optional.

POPIA applies to cookie-related processing where personal information is involved. Cookies used for direct marketing or non-essential tracking will not be deployed on the basis of assumed consent alone, especially where unsolicited electronic direct marketing is involved; South African guidance distinguishes between essential cookies and cookies used for marketing purposes.

DisputeSolve therefore uses a cookie notice or cookie management tool that distinguishes between essential cookies and optional cookies, and that records user choices where consent is required. Browser settings may also allow users to block some cookies, although doing so may affect platform functionality.

7. Direct marketing

DisputeSolve may only send direct marketing communications in a manner permitted by POPIA. Electronic direct marketing, including marketing by email, SMS or similar electronic channels, generally requires consent unless the recipient is an existing customer and the statutory conditions for approaching that customer are satisfied.

Every marketing communication will provide a clear and simple opportunity to opt out of future marketing. DisputeSolve will maintain suppression or opt-out records so that objections and withdrawals of consent are respected.

8. Disclosure of personal information

DisputeSolve may disclose personal information to employees, contractors, operators, professional advisers, payment processors, hosting providers, cloud service providers, analytics providers, dispute-resolution experts, regulators, courts, law-enforcement bodies, or other recipients where disclosure is necessary for a lawful purpose and adequately protected.

Where a third party processes personal information on behalf of DisputeSolve, that third party acts as an operator and must process the information only with the knowledge or authorisation of DisputeSolve, keep

it confidential, and maintain appropriate security measures. POPIA requires responsible parties to ensure that operators establish and maintain appropriate safeguards by contract or other binding arrangement. DisputeSolve will have a written agreement in place with every operator.

DisputeSolve will not sell personal information. Nor will it disclose personal information to unrelated third parties for their independent marketing purposes without a lawful basis and, where required, the data subject's consent.

9. Cross-border transfers

DisputeSolve may store or process personal information outside South Africa, for example through cloud hosting, software-as-a-service providers, backup systems or cross-border service providers. POPIA permits cross-border transfers only in specified circumstances, including where the recipient is subject to a law, binding corporate rules or binding agreement that provides an adequate level of protection, where the transfer is necessary for performance of a contract, where the data subject consents, or where another recognised exception applies.

Where cross-border transfers occur, DisputeSolve will take reasonable steps to verify the recipient's safeguards and ensure that contractual protections are in place.

10. Security safeguards

DisputeSolve will take appropriate, reasonable technical and organisational measures to prevent loss of, damage to, or unauthorised destruction of personal information and unlawful access to or processing of personal information. These measures may include access control, encryption, secure hosting, password management, logging, backups, role-based permissions, staff confidentiality obligations, vendor due diligence and incident response procedures.

No system can be guaranteed to be completely secure. Users also have responsibilities, including maintaining the confidentiality of login credentials and notifying DisputeSolve promptly if they suspect unauthorised access to their account.

11. Security compromise notifications

If there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, DisputeSolve must notify the Information Regulator and the affected data subjects as soon as reasonably possible, subject to any lawful limitations. South African guidance emphasises that POPIA does not create a materiality threshold before notification duties arise.

Security compromise notices will contain sufficient information to allow affected persons to take protective steps, as contemplated in section 22 of POPIA and the Information Regulator's guidance on compromise notifications.

12. Retention and deletion

DisputeSolve will retain personal information only for as long as reasonably necessary to fulfil the purpose for which it was collected, to comply with legal obligations, to resolve disputes, to enforce agreements, to maintain lawful records, or for another lawful retention basis recognised by POPIA. Different categories of records may be retained for different periods depending on legal, contractual and operational requirements.

When personal information is no longer required, DisputeSolve will securely delete, destroy or de-identify it, unless the law requires continued retention.

13. Data subject rights

Subject to POPIA and any applicable limitations, data subjects may have the right to:

- request confirmation of whether DisputeSolve holds personal information about them;
- request access to their personal information, generally through PAIA procedures where applicable;
- request correction, updating or deletion of inaccurate, irrelevant, excessive, out-of-date, incomplete, misleading or unlawfully obtained information;
- object, on reasonable grounds, to certain processing;
- object to direct marketing;
- withdraw consent where processing is based on consent, subject to the lawfulness of prior processing;
- lodge a complaint with the Information Regulator.

DisputeSolve may require proof of identity before acting on a request. Some requests may be refused or limited where the law permits this, including to protect the rights of other persons or preserve legally privileged information.

14. Accuracy and user responsibilities

DisputeSolve will take reasonably practicable steps to ensure that personal information is complete, accurate, not misleading and updated where necessary. Users should notify DisputeSolve if their details change or if information supplied through the platform is inaccurate.

Where a user submits personal information about another person, the user warrants that there is a lawful basis to do so and that any necessary notice or consent has been obtained where required by law. This is especially important in dispute-resolution contexts where large volumes of third-party information may be uploaded.

15. Children's information and special personal information

DisputeSolve does not intentionally solicit personal information from children unless this is necessary for a lawful service or dispute-related purpose and the processing is permitted by law. Where consent from a competent person is required, DisputeSolve will obtain it before processing a child's personal information.

Special personal information will only be processed where a lawful justification exists under POPIA and appropriate safeguards are implemented.

16. Third-party websites and services

The website or platform may contain links to third-party websites, software, payment systems or services. DisputeSolve is not responsible for the privacy practices of independent third parties, and users should review the privacy policies applicable to those third-party services.

17. PAIA manual and access to records

Because DisputeSolve is a private body, it maintains a current PAIA manual in terms of section 51 of PAIA and make it available on its website and through the other channels required by law. The PAIA manual explains how records may be requested and is aligned with this Privacy Policy and with current contact details.

A privacy policy does not replace the PAIA manual. Requests for access to records may need to be made in accordance with PAIA, including where the requested records contain personal information.

18. Complaints and contact details

Questions, objections, requests or complaints about this Privacy Policy or about personal information processing may be sent to popi@disputesolve.com.

A data subject may also lodge a complaint with the Information Regulator of South Africa through the Regulator's prescribed channels.

19. Changes to this policy

DisputeSolve may amend this Privacy Policy from time to time to reflect changes in law, guidance, technology, service offerings or internal processes.