



WHISTLE BLOWERS PTY LTD PRIVACY POLICY STATEMENT

1. INTRODUCTION

Whistle Blowers (Pty) Ltd understands the critical importance of protecting your personal data.

This Privacy Policy Statement sets out how Whistle Blowers (Pty) Ltd manages data regarding the users of its website and data submitted by users using its website forms and mobile applications.

This policy also represents the commitment of Whistle Blowers (Pty) Ltd to compliance with its obligations under South Africa's Protection of Personal Information Act 4 of 2013 (POPIA) and the General Data Protection Regulation (GDPR) European Union (EU) 2016/679, which is a regulation in EU law on data protection and privacy for all individuals within the European Union.

From here on in this document we refer to our company more simply as 'Whistle Blowers'.

Whistle Blowers provides an ethics hotline service that guarantees your anonymity if you use our communication channels to make a report of unethical conduct in an organisation that subscribes to this service.

Some of our data privacy processes apply to all parties that interact with Whistle Blowers, while certain special provisions apply to those using our channels on an anonymous and confidential basis to report unethical conduct involving or affecting any Whistle Blowers clients who subscribe to our service.

2. THE DATA PRIVACY OF THOSE WHO REPORT UNETHICAL CONDUCT USING OUR ETHICS HOTLINE

Whistle Blowers receives and processes information received in reports made to its ethics hotline, and after processing transfers the substance of these reports to the relevant subscribing client organisation. In this section, the personal data privacy processes applied by Whistle Blowers to reports made to our ethics hotline on an anonymous and on a non-anonymous basis are explained. In providing this ethics hotline service, Whistle Blowers is an operator on behalf of the subscribing organisation.

2.1 Data privacy of those who report unethical conduct using the ethics hotline on an anonymous or confidential basis

If you are using our ethics hotline service to make a report of unethical conduct, you need to be able to interact with Whistle Blowers in full confidence that your identity will never be known to Whistle Blowers unless you choose to disclose this to us.

If you choose to disclose your identity to us, we will keep your identity in the strictest confidence and will never disclose this to your employer or to the organisation concerned if you are not their employee.

We do not use cookies or other technology tools that could enable your identification when you browse our website or enter information into our webforms.

The only data from you that we process is data you specifically choose to give us when you make a report.

You do not need to provide any personal information in order to access information on our website or make a report using our web-based form or mobile application.

When you make a report in order to have attention given to suspected or known wrongdoing affecting one of our client organisations, we store the information you provide to us using the highest level of data security.

When we report the information you have provided to us to our client, this report has been subject to a rigorous anonymisation process that removes any identifying personal data that could reveal your identity.

This anonymised report is sent only to the people that the organisation concerned have entrusted with the responsibility of receiving and responding to anonymous and confidential reports of unethical activity.

The organisation concerned may share the anonymised report with a third party such as investigators or auditors, but we will never reveal information about your identity to such third parties.

2.2 Data privacy of those who report unethical conduct using the ethics hotline on an open, non-confidential named basis

Notwithstanding the unequivocal commitment to the anonymity and confidentiality of whistleblowers using the Whistle Blowers ethics hotline as set out in 2.1, there are instances in which reports are made on a voluntarily open, non-confidential named basis, or when whistleblowers choose during the course of the reporting process to change their report from anonymous to open.

These will include:

- Complainants to companies who need to provide their contact details in order for their complaints to be investigated, and so explicitly agree to our communication of their contact details, in conjunction with their report, to the company concerned.
- Whistleblowers who have made their reports to Whistle Blowers on an anonymous basis or in confidence and who subsequently revise their request for anonymity or confidentiality and agree to the disclosure of their personal information to the organisation concerned.
- With the express permission of those detailed here in section 2.2, their personal contact information will be conveyed to the organisation concerned in order to facilitate the progress and conclusion of an investigation or matter.

In this section we have addressed the two different ways in which data received via the Whistle Blowers ethics hotline is processed.

In both instances described in 2.1 and 2.2 above, the organisation that is the applicable client of Whistle Blowers is contractually responsible for ensuring their compliance with applicable laws in relation to all processing of personal information received via reports.

You can also be assured that:

- It is our contractual obligation as an operator providing an ethics hotline service to subscribing organisations that Whistle Blowers implements and maintains appropriate and reasonable technical and organisational measures to protect the loss, damage, unauthorised destruction and unlawful access or processing of personal information.
- Whistle Blowers' IT infrastructure provides for the electronic maintenance of all data. All data is blowfish encrypted (one of the highest forms of encryption). Calls are recorded and can only be replayed through the playback station with password access, on site. Offsite copies are also encryption enabled. This cannot be disabled and ensures that all data sent offsite, both when drive swapping and when transferring data over a VPN/WAN/Internet connection, is secured.
- Whistle Blowers is contractually committed to its clients to provide its service in accordance with the ethics hotline industry prescribed level as set out in the Safeline-EX Standard for External Whistle-blowing Hotline Service Providers. This includes a commitment to maintaining best-practice norms and standards as derived from international practices in terms of the provision of an independent, external safe reporting facility for organisations.
- Whistle Blowers is certified annually by The Ethics Institute against the Safeline-EX Standard and proof of certification is available on request using the contact details at the end of this document.

3. WHAT PERSONAL DATA WE DO AND DO NOT COLLECT

Regardless of the reason for and the method of your interaction with us, we do not collect any data that can be directly or indirectly linked to your identity, unless you choose to submit this.

We never collect any so-called 'sensitive personal information' including information relating to your health, religion, political beliefs, race or sexual orientation, except if you voluntarily share this information with us or unless we are required to do so by law.

If we link other data with your personal data, we will in keeping with legislation treat that linked data as personal data.

If you are wanting us to contact you in response to a business enquiry (where an organisation is interested in subscribing to our service and you are a representative of that business) and accordingly enter your name and contact details into our 'Contact Us' webform asking us to get in touch with you, we will collect that information and use it to follow up on your request.

We do collect data that tells us about the number of visits to our website and the number of times each page is visited, to help us monitor our website performance. This data cannot be linked to the identity of any visitor to our website.

Our third-party service providers have no access to information that you choose to submit to Whistle Blowers using our webforms and application. Even where our data is backed up and stored off-site, it is blowfish encryption enabled and fully secure.

4. HOW WE COLLECT PERSONAL DATA

As will most businesses, we collect personal data, specifically names, contact details, company details and job titles, in order to undertake the commercial operations and dealings of Whistle Blowers. This does not extend to those who use our ethics hotline to make anonymous reports of unethical activity unless you choose to provide this information voluntarily.

In order to undertake business with potential clients and existing clients and to maintain communications with stakeholders other than those using our ethics hotline to make reports, we may from time to time collect personal data in a variety of ways including when:

- There is communication between individuals communicating with us for non-hotline reporting reasons and any of our representatives
- We respond to business enquiries and requests
- We get feedback from clients about our service
- You subscribe to a mailing list or register for an event managed by Whistle Blowers
- We market our services
- People apply for employment with us

- We undertake our administrative and business functions (e.g. procurement, invoicing and payments).

In respect of non-hotline reporting contacts, we may also collect personal data from third party sources, generally to assist our marketing efforts, but only to the extent permitted by applicable laws.

5. PURPOSES FOR WHICH WE COLLECT AND USE PERSONAL DATA

We collect and use personal data with exception in respect of individuals in the course of using our ethics hotline to report unethical activity on an anonymous and confidential basis in order to:

- Send communications to you
- Establish, manage, and maintain our business relationships
- Respond to enquiries and requests
- Develop, provide, and improve our services and solutions
- Inform you about our services and solutions
- Obtain feedback from you on our services and solutions
- Conduct administrative and business functions
- Update our records and keep contact details up to date
- Enable you to effectively use and to improve our websites
- Compile website usage statistics
- Enable you to subscribe to newsletters and mailing lists
- Enable you to register for Whistle Blowers (Pty) Ltd.'s events, workshops and seminars
- Recruit staff
- Assess the performance of our websites and to improve their operation
- Process and respond to privacy questions, concerns and complaints
- Fulfil legal and contractual obligations.

6. SHARING DATA WITH OTHER ORGANISATIONS

The personal data we hold, with the exception of that relating to those using our ethics hotline for anonymous and confidential reporting of unethical activity, may be shared by us with third parties who are themselves required to comply with the privacy legislation as set out in the introduction to this policy, under the following circumstances:

- In connection with any joint venture, merger, the sale of company assets, consolidation or restructuring, financing, or acquisition of all or a portion of our business by or to another company.
- In response to a request for information by a competent authority in accordance with, or required by any applicable law, regulation or legal process.
- Where necessary to comply with judicial proceedings, court orders or government orders.
- To protect the rights, property or safety of Whistle Blowers (Pty) Ltd, its business partners, you, or others, or as otherwise required by applicable law.
- Where you consent to the sharing of your personal data.

7. ONWARD TRANSFERS OF DATA

Whistle Blowers (Pty) Ltd may transfer your personal data to organisations within the Republic of South Africa as well as other countries where we do business in connection with for the purposes identified above and in accordance with this Privacy Statement.

Where we transfer your personal data from a location within the European Economic Area or Switzerland to a country outside the EEA or Switzerland and that country does not provide a level of protection for personal data which the European Commission deems adequate, we adhere to the standard contractual clauses (SCCs) approved by the Commission, and applicable data protection laws in the EEA which give you the following rights:

- Where Whistle Blowers (Pty) Ltd processes your personal data based on your consent, you may withdraw your consent at any time for future processing.
- You may request access to and correction of your personal data which is held by us at any time.
- You may object to the processing of your personal data at any time.
- You may lodge a complaint with a data protection authority if you believe that your rights relating to the protection of your personal data have been breached or that your personal data has been compromised.
- Where Whistle Blowers (Pty) Ltd transfers your personal data to third parties, Whistle Blowers (Pty) Ltd requires those third parties to sign agreements which include the SCCs (or other data transfer mechanism approved by the Commission).

8. SECURITY OF YOUR PERSONAL DATA

Whistle Blowers (Pty) Ltd is committed to protecting your personal data from misuse, loss, unauthorised access, modification or disclosure by using a combination of physical, administrative and technical safeguards and contractually requiring that third parties to whom we disclose your personal data do the same.

When you submit or post personal data online, you should be aware that the internet is not completely secure. Whistle Blowers (Pty) Ltd cannot guarantee the security of any personal data that you submit or post online but it can assure you that in its own collection and processing of this data that your privacy rights will always be honoured and protected.

As previously stated, Whistle Blowers' IT infrastructure provides for the electronic maintenance of all data. All data is blowfish encrypted (one of the highest forms of encryption). Calls are recorded and can only be replayed through the playback station with password access, on site. Offsite copies are also encryption enabled. This cannot be disabled and ensures that all data sent offsite, both when drive swapping and when transferring data over a VPN/WAN/Internet connection, is secured.

9. DIRECT MARKETING

Even when you have agreed to receive marketing information from us, you may opt out of receiving marketing materials from us at any time and manage your communication preferences by sending an email to admin@whistleblowing.co.za or writing to us at Whistle Blowers (Pty) Ltd, PO Box 51006, Musgrave 4062, Durban, South Africa, including your details and a description of the marketing material you no longer wish to receive from us. We will comply with your request as soon as is reasonably practicable.

We do not provide your personal data to unaffiliated third parties for direct marketing purposes or sell, rent, distribute or otherwise make personal data commercially available to any third party.

10. HOW YOU CAN ACCESS, CORRECT, UPDATE, BLOCK OR DELETE YOUR PERSONAL DATA

If you wish to access, correct, update, block, or delete personal data that we hold about you, please write to us using the contact details set out at the end of this Privacy Statement. We will respond within a reasonable period and, at the latest, within 30 days of the date of your request.

11. LINKS TO THIRD PARTY WEBSITES AND APPLICATIONS

Our websites may contain links to sites and applications operated by third parties. We make no representations or warranties in relation to the privacy practices of any third-party site or application, and we are not responsible for any third-party content or privacy statements. Your use of such sites and applications is subject to the relevant third-party privacy statements.

12. RETAINING YOUR PERSONAL DATA

12.1 Retention of personal data not provided via an ethics hotline report

We retain personal data for as long as is necessary to fulfil the purposes for which it was collected or to comply with legal obligations, resolve disputes, protect our assets, or enforce agreements. Depending on the purpose, retention periods will vary. The criteria we use to determine retention periods include whether we are under a legal, contractual or other obligation to retain personal data including pursuant to data retention laws, as part of an investigation or for litigation purposes; or personal data is needed to provide our solutions and services business, including performance improvement and to maintain accurate business and financial records.

12.2 Retention of personal data received via ethics hotline reports

Whistle Blowers retains all data received via ethics hotline reports, and all reports that it subsequently prepares for and submits to its clients, in accordance with the provisions of all applicable laws.

Depending upon the jurisdiction in which they operate, the contractual obligations agreed with our clients in respect of data retention and data removal vary. For more information about data retention practices in respect of different legal jurisdictions please make use of the contact details at the end of this policy.

13. CHANGES TO OUR PRIVACY STATEMENT

We may update this Privacy Statement from time to time. If we do, we will post the revised version on our website, with an updated revision date.

14. HOW TO CONTACT US

If you have any questions about how your personal data is handled by Whistle Blowers (Pty) Ltd, you have a privacy concern, or you wish to make a complaint, please contact Whistle Blowers (Pty) Ltd.'s **Director: Finance & Compliance** using the following contact details:

Email: admin@whistleblowing.co.za

Phone: +27 31 308 0600

Post: PO Box 51006, Musgrave 4062, Durban, South Africa
