

POPI



WhatsApp Policies & POPI Compliance

The involvement of the South African Information Regulator in the review of WhatsApp's amended Terms & Conditions and Privacy Policy has South Africa wondering whether WhatsApp does in fact comply with our privacy laws and specifically the Protection of Personal Information Act 4 of 2013.

So let's examine what information WhatsApp collects? WhatsApp collects the following information including but not limited to:

1. Automatically collected information:

- Usage & Log Information: Basically the users activity on the platform, how you use it, how you interact with others & businesses, the time frequency & duration of your activities including group information such as group name, group picture, group description.
- Device & Connection Information: What device & hardware you use, battery life of device, mobile network etc.
- Location Information. Precise location information from your device with your permission when you choose to use location-related features, like when you decide to share your location with your contacts or view locations nearby or locations others have shared with you
- Cookies. Cookies are used by WhatsApp to operate and provide their services, to understand how their services are being used, to remember the users choices, like language preferences etc.

2. Other Information

- Information enabling it to provide its services. to operate, provide, improve, understand, customise, support, and market services. The types of information WhatsApp receives and collects depend the users use its services.
- Users use of optional features which, if used, WhatsApp collects additional information to provide such features. Users will be notified of such collection, as appropriate. This is an example of non POPI compliance. Who deems if notification is appropriate? Does not comply with principle of Openness (see below) in POPI that a user is aware of the information being collected and the source from which it is collected. Individuals must be aware of the specific personal information held about them and the purpose to which the information is being retained. WhatsApp states that if you choose not to provide the information needed to use a feature, you will be unable to use the feature. For example, you cannot share your location with your contacts if you do not permit it to collect your location data from your device.
- The information the user provides which is account information(mobile phone number and basic information (including a profile picture, and "about" information. profile name of your choice)
- When a user uses the contact upload feature, he/she grants WhatsApp access to your device's address book, WhatsApp will access and upload the phone numbers in your address book on a regular basis, including those of both the users of WhatsApp and your other contacts. The Contact upload feature unlawful in terms of POPI. Does not meet Processing Limitation & Further Processing Limitations (see below) in terms of POPI.
- Status information, the users status as updated by the user.
- Transactions and Payment Data. If you use WhatsApp payments services, or use our Services meant for purchases or other financial transactions, it process additional information about you, including payment account and transaction information.
- In respect of business transactions, the policy states Payments on WhatsApp, which are available in select countries, enable transfers between accounts at financial institutions. Card and bank numbers are stored encrypted and in a highly-secured network. However, because financial institutions can't process transactions without receiving information related to these payments, these payments aren't end-to-end encrypted.
- When a user contacts WhatsApp for customer support or otherwise communicates with it, the user may provide it with information related to the use of their services, including copies of user's messages, any other information and how to contact the user (e.g., an email address).

3. Third-Party Information:

- Information Others Provide About You as a user. WhatsApp receives information about you from other users. The policy states that an example is, when other users you know use our Services, they may provide your phone number, name, and other information (like information from their mobile address book) just as you may provide theirs.

What are the requirements WhatsApp must comply with in terms of POPI?

The Information Regulator will no doubt review the Privacy policy in line with the eight principles of compliance of POPI, which are as follows:

4. WhatsApp has to comply with the 8 Minimum POPI Compliance Requirements.

- POPI provides 8 minimum requirements for compliance.
- **Accountability:** An organisation is accountable for the lawful processing of personal information and this duty cannot be outsourced.
- **Processing Limitation:** Organisations are required to collect only the minimum required information for their purpose. The consent of the data subject/person must be obtained ensuring that he/she knows the purpose as well as the type of information being processed.
- **Purpose Specification:** Personal information must be collected for a legitimate, lawful & specific purpose and must not be retained for longer than the required period unless it is lawful to do so.
- **Further Processing Limitation:** An organisation is obliged to prevent the processing of information in a manner that is incompatible with the purpose for which the information was collected. Generally, this limits any secondary use of personal information, for any other purpose than the purpose for which it was collected for initial processing. This includes preventing the disclosure or transfer of personal information to third parties.
- **Information Quality:** The organisation must take reasonably practical steps to ensure that personal information is complete, accurate, not misleading and updated where necessary.
- **Openness:** The organisation is required to ensure that the data subject/person is aware of the information being collected and where the information is not collected from the data Subject, the source from which it is collected. Individuals must be aware of the specific personal information held about them and the purpose to which the information is being retained.
- **Security Safeguards:** The organisation must secure the integrity and confidentiality of personal information in its possession by taking appropriate reasonable and technical measures to prevent loss, damage and unlawful access. In order to do so, it is important for the organisation to:
 - Identify all reasonably foreseeable internal and external risks to the personal information in its possession;
 - Establish safeguards such as passwords to restrict internal and external access; and
 - Regularly update the safeguards to prevent hacking.
- **Data Subject Participation:** The data subject/person is entitled to
 - An explanation of the personal information;
 - Request information about the recipients of personal information; and
 - Request deletion or correction of the personal information.
- This participation ensures that the data subject/person has some measure of influence over the processing of their personal data.

5. The Powers of the Information Regulator

- The Information Regulator is an independent body established in terms of POPI, which must be impartial and perform its function without fear, favour or prejudice.
- The Information Regulator has powers of search & seizure, to impose fines, receive complaints, issue notices, make regulations, issue codes of conduct and conduct assessments of organisation.
- The Information Regulator will monitor and enforce compliance with POPI by WhatsApp by:
 - conducting an assessment of its policies in respect of its processing of personal information either on its own accord or on request;
 - Conducting a comparison of the European Unions Policies & South African Policies to determine any differences in application (this is as a result of the European Union being governed by the General Data Protection Regulations & South Africa being governed by POPI);
 - addressing complaints lodged with the Information Regulator with regards to non-compliance by WhatsApp either through mediation or conciliation.

6. Serious Consequences & Penalties for Non-Compliance.

- Should there be interference with a data subject's/persons protection of personal information, the aggrieved party may lodge a complaint with the Information Regulator. A negotiated settlement is one of the possible outcomes of the complaints procedure. The Regulator does not require a court order to institute a fine for negligence or non-compliance in favour of the aggrieved party in terms of POPI.
- POPI further provides for civil remedies where the court may award amounts that, in its discretion, are just and equitable. Such amounts include:
 - Payment for damages as compensation for losses suffered by a data subject as a result of a breach of a provision of POPI;
 - Aggravated damages;
 - Interest; and
 - Costs on a scale as determined by the court.
- There are dire consequences for any party being convicted of an offence in terms of POPI. A maximum period of imprisonment of 10 years for Company owners & Directors, or an undisclosed maximum fine(each fine to be determined by the relevant court on a case-by-case basis) can be levied. Furthermore, the Regulator may institute administrative fines up to an amount of R10 million.

In our *prima facie* view, WhatsApp's Terms & Conditions and Privacy policies do not comply with POPI. This means that all the Facebook controlled companies & platforms including Facebook and Instagram, in addition to WhatsApp will need to bring their Terms & Conditions and Privacy policies in line with South African Privacy law or face the consequences.

Published by



Diana Schwarz

Admitted Attorney with 15years PQE/Social Media Law Expert/ Labour Law Specialist / Experienced Commercial Litigator.

www.dianaschwarzattorneys.co.za



DIANA SCHWARZ ATTORNEYS